MEETING AGENDA

BCIT BOARD OF GOVERNORS – OPEN

Wednesday December 3, 2025, 3700 Willingdon, Burnaby, BC

- Open Meeting begins: 2:45 to 3:50 p.m., SE02 - Town Square A/B

- Join the meeting now; Mtg ID: 281 365 159 362; Passcode: wr9xi2sC
- Telephone: +1 647-794-1704,,245203181#, ID: 245 203 181#

Board:
Mike Bonshor, Chair
Don Matthew, Vice Chair
Corry Anderson-Fennell
Cora Bell
Catherine Boivie
Annabelle Donovan
Bobby Davidson
Noor Esmail
Zahra Esmail
Brooks Patterson
Carla Reid
Stepan Vdovine
Claire Wang

Ex Officio:
Jeffrey Zabudsky, President
Shawna Waberi, Education Council Chair

In Attendance:
Tanya Buschau, Advisor, Respect, Diversity & Inclusion (#6.4)
Raimonda De Zen, Dir. Enterprise Risk & Internal Audit
Jennifer Figner, Provost & VP, Academic
Chris Hudson, VP, People, Culture & Inclusion
Cynthia Petrie, VP, External
Navida Suleman, CFO and VP, Administration
Barbara Kader, EA, Governance

Regrets:
Colin Jones, Board Member

	Item		Presenter	Page
1.	**Call to Order and Introductory Remarks** *BCIT acknowledges that its campuses are located on unceded Indigenous land belonging to the Coast Salish Peoples, including the territories of the xʷməθkwəy̓əm (Musqueam), Sḵwx̱wú7mesh (Squamish) Nations*	2:45	Chair	-
2.	**Disclosure of Conflict of Interest**	2:47	Chair	4
3.	**Approval of Agenda/Consent Agenda** *(subject to request for discussion)* 3.1 Adopt Agenda 3.2 Minutes October 7, 2025 3.3 Education Council Report 3.4 Governance Committee Report 3.5 Institute Report 3.6 Public Interest Disclosure and Protection Annual Report (FY2024/25) ***MOTION:*** *THAT the Board of Governors approves the Agenda/Consent Agenda for the Open Board of Governors meeting held on December 3, 2025.*	2:50	Chair	3 5 11 14 15 28
4.	**Board Chair's Comments**	2:55	Chair	30
5.	**President's Comments** 5.1 President's Activities	3:05	J. Zabudsky	30 31

	Item		Presenter	Page
6.	**Policies and Procedures** 6.1 Acceptable Use of Information Technology – Policy #3501, and Information Security – Policy #3502. ***MOTION:*** *THAT the Board of Governors approve revisions to the Acceptable Use of Information Technology - Policy #3501, and the Information Security – Policy #3502.* 6.2 Admissions and Recognition of Prior Learning – Procedure #5003-PR1 ***MOTION:*** *THAT the Board of Governors approves the revised Admissions and Recognition of Prior Learning - Procedure - 5003-PR1.* 6.3 Recording in the Classroom – Policy #5201 ***MOTION:*** *THAT the Board of Governors approves the revised Recording in the Classroom - Policy #5201 and Recording in the Classroom - Procedure - 5201-PR1.* 6.4 Prevention of Discrimination, Harassment, and Bullying – Policy #7507, and Harassment and Discrimination – Procedures #7507-PR1 ***MOTION:*** *THAT the Board of Governors approves the revised Prevention of Discrimination, Harassment, and Bullying - Policy #7507, and Procedure #7507-PR1.*	3:20	D. Matthew / N. Suleman C. Anderson-Fennell / S. Waberi " " C. Wang / C. Hudson	35 129 145 168
7.	**Academic** 7.1 New Programs: • Certificate in Professional Remotely Piloted Aircraft Systems • Diploma in Construction Management ***MOTION:*** *THAT the Board of Governors approves the new programs: Certificate in Professional Remotely Piloted Aircraft Systems, and Diploma in Construction Management*	3:45	S. Waberi	223
8.	**Next Meeting and Conclusion** February 24, 2026	3:50	-	242

Board of Governors Open Meeting – December 3, 2025
1.0 Call to Order and Introductory Remarks
4.0 Approval of Agenda/Consent Agenda

MOTION: THAT the Board of Governors approve the Agenda/Consent Agenda for the Open Board of Governors meeting held on December 3, 2025.

List of Motions for Approval

6.1 THAT the Board of Governors approves revisions to the *Acceptable Use of Information Technology - Policy #3501, and the Information Security – Policy #3502, and the retirement of the Information Security Procedure – Procedure #3502.*

6.2 THAT the Board of Governors approves the revised *Admissions and Recognition of Prior Learning - #5003-PR1 Procedure.*

6.3 THAT the Board of Governors approves the revised *Recording in the Classroom - #5201 and Recording in the Classroom Procedure #5201-PR1.*

6.4 THAT the Board of Governors approves the revised *Prevention of Discrimination, Harassment, and Bullying - Policy #7507, and Procedure #7507-PR1*.

7.1 THAT the Board of Governors approves the following new programs: *Certificate in Professional Remotely Piloted Aircraft Systems, and Diploma in Construction Management*.

INFORMATION NOTE
November 26, 2025

PREPARED FOR: Board of Governors

ISSUE: Disclosure of Conflict of Interest

SUMMARY:

A *Disclosure of Conflict of Interest* provides an opportunity for Governors to announce if they have a conflict with any of the open and/or closed board meeting agenda item(s).

Governors should refer to the *Board of Governors Bylaws, Part IV – Code of Conduct and Conflict of Interest (page 14)*, and the *Board of Governors' Governance Manual – section 8, Governor Conflict of Interest (page 21).*

The bylaws and manual can be found here.

MEETING MINUTES

BCIT BOARD OF GOVERNORS - OPEN

Tuesday October 7, 2025, 1:02 to 2:06 p.m.

Board:
Mike Bonshor, Chair
Don Matthew, Vice Chair
Corry Anderson-Fennell *(virtual)*
Cora Bell
Catherine Boivie
Annabelle Donovan
Bobby Davidson *(virtual)*
Noor Esmail
Zahra Esmail *(virtual)*
Colin Jones
Brooks Patterson
Carla Reid
Stepan Vdovine *(virtual)*
Claire Wang

Ex Officio:
Jeffrey Zabudsky, President
Shawna Waberi, Education Council Chair

In Attendance:
Raimonda De Zen, Dir. Enterprise Risk & Internal Audit
Jennifer Figner, Provost & VP, Academic
Chris Hudson, VP, People, Culture & Inclusion
Simon Lam, (#6.2) Dir., Respect, Diversity & Inclusion
Wendy Lebreton, Dir., Land Asset Management
Cynthia Petrie, VP, External
Navida Suleman, CFO and VP, Administration
Barbara Kader, EA, Governance

A quorum was present.

1.0 Call to Order and Introductory Remarks

The Chair acknowledged that BCIT campuses are located on unceded Indigenous land belonging to the Coast Salish Peoples, including the territories of the xʷməθkwəy̓əm (Musqueam), Sə̓lílwətaʔ/Selilwitulh (Tsleil-Waututh) and Skwxwú7mesh (Squamish) Nations.

2.0 Declaration of Conflict of Interest

Distributed material: Information Note

No declarations were received.

3.0 Governor Appointments

3.1 Introductions, Profiles and Oaths of Office

Distributed material: Information Note

Introductions were made from the new governors (A. Donovan, Z. Esmail, B. Patterson). Each Oath was previously signed and received.

4.0 Approval of Agenda/Consent Agenda

All reports were received as read. An amendment was made to move item *4.5 Sexualized Violence Annual Report 2024/25* to 6.2. A request to add an agenda item was made. It was decided that the addition would be discussed in the In Camera session after the Closed meeting.

IT IS HEREBY RESOLVED, SECONDED AND CARRIED THAT the Board of Governors approves the *amended* Agenda/Consent Agenda for the Open Board of Governors meeting held on June 23, 2025.

4.1 Adopt Agenda
Distributed material: Agenda

4.2 Minutes June 23, 2025
Distributed material: Meeting Minutes

4.3 Education Council Report
Distributed material: Information Note

4.4 Governance Committee Report
Distributed material: Information Note

4.5 Institute Report
Distributed material: Information Note

4.6 Student Association President's Report
None provided – no verbal update

4.7 Student Representative's Report
None provided – no verbal update

5.0 Board Chair's Comments

The Board Chair reported that he had a tour of the Broadcasting Centre (School of Business + Media).

He was impressed by the team's dedication and their work in such a rapidly evolving field, it's clear they'll continue to adapt and remain relevant. The school is committed to staying current, fully subscribed in most areas, and focused on maintaining excellence in this dynamic sector of communication.

6.0 President's Report

The President introduced Wendy Lebreton (Director, Land Asset Management) and acknowledged the new Governors.

6.1 President's Activities
Distributed material: Information Note

The President highlighted key activities from his report previously circulated.

He reported that during the summer, activities included visiting each of the five municipalities with campuses, engaging in formal presentations to Council and mayors. Presentations have been completed in Burnaby and Richmond, while North

Vancouver, Vancouver, and Delta are being scheduled. The tours provided an opportunity to discuss BCIT's initiatives to support local communities. In Richmond, the new biomanufacturing centre at the aerospace campus was introduced to council members, who were invited for upcoming tours.

Additionally, a proposal has been made for a pedestrian bridge connecting Lansdowne SkyTrain station to the Aerospace Campus, aiming to improve access for students and the adjacent Burkeville community. Although not a primary priority, the project is being considered for future development.

Subsequent meetings involved the minister visiting BCIT's Marine campus, discussing institutional challenges and the impact of the Bridge Watch Rating program. The minister also participated in industry engagement sessions, including two visits to observe shipbuilding and manufactured modular construction projects. Both companies highlighted their collaboration with BCIT and contributions to education and workforce training.

Notable events also included a Burnaby Campus tour for the Federal Minister of Housing, focusing on the student housing project. The tour showcased modern mass timber construction techniques and net zero housing initiatives, with potential for further federal investment in student housing to benefit both students and the broader community.

The visit was productive, highlighting the innovative mass timber construction approach, panelized and assembled on campus, and work in net zero housing and master timber micro credentials. The Minister expressed interest in returning specifically to see this new construction method.

The President will be attending Polytechnics Canada's National Strategy Group Meetings in Ottawa in late October and will be bringing a CEO from a Vancouver mass timber design company whose business aligns with the federal government's focus on housing innovation.

6.2 Sexualized Violence Annual Report 2024/25
Distributed material: Information Note

A report was provided on sexualized violence prevention within the BCIT community. This topic is a key priority for both the Deputy Minister and the Minister.

BCIT remains committed to a comprehensive approach for addressing sexual violence and misconduct. The ministry introduced new proposed legislation, which is currently being reviewed; initial assessments indicate current BCIT practices are aligned with the new legislation and new measures will strengthen sector-wide efforts.

Over the past year, BCIT has prioritised progression and education, updating campus safety and course content for faculty, staff, and students. Preparation has begun on a awareness campaign for housing students, aiming to launch by year's end or early next year. New resources and handouts will support faculty and staff in assisting students, with plans to roll these out by end of next term. The website will be updated later this year and fully revamped next year to improve support and accountability around preventing sexualized violence on campus. Last year, an anonymous online

reporting tool was introduced, allowing community members to report incidents confidentially.

This policy addressing sexual violence, along with its accompanying procedures, will be reviewed. BCIT is committed to conducting a thorough consultation process, in which student input and community feedback will play a crucial role. Based on the information gathered, further revisions and enhancements as necessary will be made.

Management answered questions on how BCIT tracks incidents of sexualized violence on campus and where can details about how this information is recorded and what it means be found.

Reports are received through various channels, as individuals may choose to approach safety and security; student success; respect, diversity and inclusion; or human resources based on their preferences. These reports are tracked and collected using different methods. A small group meets regularly to review cases that arise. Efforts are underway to ensure data accuracy and improve tracking processes, with plans over the coming weeks and months to capture all relevant information at BCIT. The reporting avenues include both disclosures and formal reports.

BCIT aims to respect the preferences of individuals affected by sexual violence; some may prefer confidentiality and only seek support without disclosure. Their wishes are honoured and their experiences may not be included in reported statistics. However, the community is encouraged to seek assistance or report concerns, particularly in serious cases, while maintaining a balance between respecting individual choices and ensuring campus safety.

Management provided a summary of training sessions extended to all staff.

7.0 Finance

7.1 Financial Information Act – Annual Report Submission (SOFI)

Distributed material: Decision Note

Management reported that previously we were able to file documents to meet the ministry's September 30 deadline after the audit finance reviewed the report with pending board approval. Going forward, pending board approval will no longer be required, the board will be requested to formally delegate approval authority to the committee to facilitate timely filing and compliance.

IT IS HEREBY RESOLVED, SECONDED AND CARRIED THAT the Board of Governors approves the FY2024/25 Statement of Financial Information.

8.0 Policies and Procedures

8.1 Fraud – Policy #1200

Distributed material: Decision Note

Management reported that edits made to the policy are minor and were completed with the assistance of the Policy Management Office. There have been no material changes to the original intent of the policy. Revisions to change in oversight responsibilities: oversight remains with Internal Audit until the program is fully implemented, at which time it will be transferred to the Enterprise Risk Management team.

Management reported that BCIT has a code of conduct policy that addresses conflicts of interest. When new policies are drafted or existing ones revised, all related organizational policies are reviewed for connections and ensure they're reflected in the latest versions. The Policy Management Office supports this process by offering guidance and helping identify links between policies. Stakeholders are also involved during consultations for new or revised policies to consider relevant connections and feedback.

IT IS HEREBY RESOLVED, SECONDED AND CARRIED THAT Board of Governors approves the revised Fraud - Policy #1200.

8.2 Program Review – Policy #5402 and Program Review Process Procedure - #5402-PR1

Distributed material: Decision Note, Presentation, Report

Management reported that revisions comprised to simplify language and readability. References to the ministry has been more generic, should the Ministry titles change with leadership.

IT IS HEREBY RESOLVED, SECONDED AND CARRIED THAT Board of Governors approves the revised Program Review - Policy #5402 and Program Review Process - Procedure - #5402-PR1.

9.0 Academic

9.1 New Programs:

- Advanced Certificate in Bridging Medical Radiography
- Associate Certificate in Artificial Intelligence Management
- Associate Certificate in Business Data Management
- Associate Certificate in Business Intelligence

Distributed material: Decision Note, Reports

The Education Council Chair highlighted each of the new certificates, reporting on the target audiences where curriculums required prior knowledge and experience.

An associate certificate requires a minimum of 15 credits, and the rigour is traditionally at the level of first-year post-secondary study. An advanced certificate requires at least 24 credits, with a diploma or a degree for entry, and is comparable to third-year post-secondary level or higher.

BCIT offers flexible learning options, available during evenings and weekends to meet demand. Full enrolment is expected, if interest grows, additional sessions will be offered.

IT IS HEREBY RESOLVED, SECONDED AND CARRIED THAT the Board of Governors approves the new programs: Advanced Certificate in Bridging Medical Radiography; Associate Certificate in Artificial Intelligence Management; Associate Certificate in Business Data Management; Associate Certificate in Business Intelligence.

10.0 Governance

10.1 Committee Memberships
Distributed material: Decision Note

The Committee Chair provided a summary of the membership revisions.

IT IS HEREBY RESOLVED, SECONDED AND CARRIED THAT the Board of Governors approves the following Committee membership revisions, effective October 7, 2025:

- Audit and Finance Committee: to remove Bob Enns (retired), to add Brooks Patterson
- Human Resources Committee: to remove Catherine Boivie and Don Matthew; to add Annabelle Donovan and Brooks Patterson
- Governance Committee: to add Colin Jones and Shawna Waberi
- Tributes Committee: to remove Corry Anderson-Fennell; to add Zahra Esmail

11.0 Next Meeting and Conclusion

The next Board of Governors meeting will be held on December 3, 2025 at 1:00 p.m. The open meeting concluded at 2:06 p.m.

Mike Bonshor, Chair

INFORMATION NOTE
November 20, 2025

PREPARED FOR: Board of Governors

PREPARED BY: Shawna Waberi, Education Council Chair

ISSUE: Education Council Update

SUMMARY:

Education Council (EdCo) is bringing forward two policies and two programs for Board approval:

- Admissions and Recognition of Prior Learning – Procedure #5003-PR1
- Recording in the Classroom - Policy #5201 and Recording in the Classroom - Procedure - #5201-PR1
- Proposals for new programs:
    - Certificate Professional Remotely Piloted Aircraft Systems
    - Diploma in Construction Management

EdCo met on November 19, 2025, where they reviewed and discussed the items listed below.

EdCo Business Report from Shawna Waberi, EdCo Chair:

- Shawna opened the meeting with an intentional land acknowledgement and highlighted the importance of education in the Truth and Reconciliation Commission of Canada: Calls to Action report. She shared call to action 57, which refers to professional development and training for public servants, reminding council that advancing Indigenization and decolonization in the classroom, requires educators to first become students themselves.
- Shawna attended the BC College and Institutes Academic Governance Council: Community of Practice meeting on October 24. Generative AI dominated much of the informal discussion, with consensus that the rapid change and increased roll-out of various AI-tools makes it a challenge to develop policy to protect academic integrity and education quality.

Program Reviews:

One Year Status Reports

- Certificate in Security Systems Technician, SoC&E: Most items are complete with work on marketing to support increased student enrollment, and hardware/software procurement ongoing.

Report from Student Association – Pratham Pannu, Student Association VP Student Experience

- Fall term SA and Club activities continued to provide opportunities for student collaboration and engagement across all campuses and schools. Highlights include Recharge de-stress, Halloween activities and Career-Industry networking events. As of November 1, over 13,000 students have participated in BCITSA events.
- Food pantry numbers are at peak levels with an average of 135 weekly student visitors.
- The BCITSA will hold a referendum in February 2026 to seek student approval in relocate unused BCITSA funds and increase student fees by $4/year for the next three years to expand the budget for SA event and Club event funding.

Programming Committee, Michelle House-Kokan, Chair:

- Two new program proposals were approved to bring forward to EdCo and the Board (see Decision Note).

Education Policy Committee, Trevor Lord, Vice Chair:

- Policy committee guidelines document will be implemented in 2026 to improve transparency and consistency in the work completed by policy working groups.
- The Admissions procedure 5003-PR1 was amended and approved to bring forward to EdCo and the Board. As well the Recording in the Classroom policy 5201 and procedure 5201-PR1 has gone through a thorough review with updates (see Decision Notes).
- Policy Updates: Progress on various policies including:
    - P5103 Student Evaluation and P5104 Student Code of Academic Integrity will align and integrate as much as possible with the BCIT Academic Integrity working group.
    - P5405 Program Suspension and Cancellation will progress in the fall.

Educational Technology and Learning Design Committee (ETLDC), Erika Ram, Chair:

- The committee will focus on five areas in the coming year:
    - Generative AI, Policy & Governance
    - Identify new EdTech tool needs' work with ETS/IAPO
    - Academic Integrity Tools
    - Chat platforms/MS Teams student license/LTI
    - Online Course & Resources Retention Policy

- The committee provided extensive feedback to the community review of Policy 3501 Acceptable Use of Information Technology.

Other Business:

- A council member shared that Northwestern Polytechnic in Alberta is closing its Fairview campus at the end of the 2025-26 academic year, resulting in the suspension or cancellation of many trades and technology programs, including the motorcycle technician training program. BCIT will be the only remaining institute in Western Canada to offer training in this field.

Questions are welcomed from the Board of Governors.

INFORMATION NOTE
November 19, 2025

PREPARED FOR: Board of Governors

ISSUE: Governance Committee Report

SUMMARY:

On November 18, 2025, the Governance Committee convened to review and approve items scheduled for presentation at the Board meeting on December 3, 2025.

Items for Approval

Policy Revisions – the Committee reviewed changes to both policies and will request board approval on December 3.

- **Admissions and Recognition of Prior Learning – Policy #5003**, and **Recording in the Classroom – Policy #5201**

INFORMATION NOTE
November 23, 2025

PREPARED FOR: Board of Governors

ISSUE: Institute Report

The report summarizes key activities from September to November 2025 that advance BCIT's four Strategic Plan commitments.

- **TRANSFORM TEACHING AND LEARNING**
- **CATALYZE DIGITAL TRNSFORMATION**
- **FOSTER VIBRANT COMMUNITIES**
- **ENRICH PARTNER EXPERIENCES**

TRANSFORM TEACHING AND LEARNING

Applied Research - Centre for Applied Research and Innovation (CARI)

- BCIT Smart Microgrid Applied Research Team (SMART) researcher Dr. Moein Manbachi has been awarded 1.21M for two projects. First, the Research and Development cybersecurity project, *Digital Twin Platform for Critical Infrastructure Cybersecurity Modeling and Assessment* in collaboration with academia, utility, and industry partners. Second, the Training cybersecurity project, *Critical Infrastructure Cybersecurity Experiential Training Program* in collaboration with BCIT schools, utility, and industry partners.

- Applied research at BCIT spans all schools and disciplines, including computing, health, business, energy, and more. Recently, Michał Aibin, Ph.D. from BCIT Computing was featured on Global News to discuss how his team utilizes technology to enhance community safety in the context of wildfires. This wildfire initiative, developed in partnership with Spexi and supported by Mitacs and National Research Council Canada / Conseil national de recherches Canada, demonstrates the tangible impact of BCIT's applied research, addressing critical challenges faced by communities.

- After earning gold at the **2024 CYBATHLON in Switzerland**, the BCIT MAKE+ team has once again achieved international recognition for its groundbreaking wheelchair, the BEAST. On September 17, the paper "BCIT's BEAST wheelchair takes on Cybathlon with power, precision, and pilot-led design" authored by Garrett Kryt, Rory Dougall, and Dr. Jaimie Borisoff was published in Science Robotics. The work highlights the engineering and innovation that powered our gold-medal success.

Institute Sustainability

- Jennie Moore, (Sustainability Director), attended the annual **Zero Waste Forum** in Istanbul from October 17 to 19. She led a **UN Habitat Youth Advisory Board** session about essential skills for sustainability leaders. The consultation's results, shared with the Associate VP Academic, highlight social media learning, managing disinformation, working with AI, leadership and communication development, and gaining practical skills credit through online self-assessment and third-party verification.

Respect, Diversity & Inclusion (RDI)

- On October 24, RDI and the **ConnectHER Hub** held a professional development day for women and gender-diverse trades faculty, featuring sessions on student conduct, de-escalation, classroom management, and plans for an employee resource group.

- BCIT was nominated for the 2025 Inclusive Culture Champion – Public Sector award at the Untapped Workplace Inclusion Awards, hosted by the Open Door Group.

- As part of BCIT's commitment to transparency on our accessibility work, we published our Accessibility Plan Annual Update for 2024/25, including physical upgrades to our campuses, delivery of events regarding accessibility, and defined working groups for our Accessibility Steering Committee.

School of Business + Media (SoBM)

Burnaby Campus (BBY), Downtown Campus (DTC)

- Eight BCIT **Graphic Design students** spent four months working with the Burnaby Fire Department, developing and prepping a booklet for print. The finished product helps promote fire safety for young children in the community.

- **Robert Jago** has joined the school as its first **Indigenous Storyteller in Residence**. He appeared on CBC Early Edition with Stephen Quinn to discuss his new role, which includes guiding students and faculty in advancing Reconciliation, Indigenous awareness and understanding, and sensitivity in storytelling and content creation.

- **General Insurance and Risk Management student teams** won first and second place in the national **C2C Challenge**. The competition tasks Canadian post-secondary students with creating risk management reports from real case studies; this year's case was a joint venture between a First Nation business and a non-Indigenous partner for a large construction project.

- **Katrina Chen**, President of AnXin Community Savings and former BC Minister of State for Child Care, spoke to Business Management students about her leadership journey.

- In partnership with the **Design Professionals of Canada (DesCan),** the school hosted the Launch! **Student Conference 2025** at the Tech Collider in DTC. The event included portfolio reviews designed for students and recent graduates who aim to pursue careers in communication design, as well as for individuals currently studying in design programs.

- Broadcast and Media students **Sophie Hansen, Emily Dineen, Lauren Accili, and Lisa Kovtun** from the TV/Video program received the esteemed **Excellence in Feature Reporting** award at the **Jack Webster Awards** for their documentary *"At What Cost? The Legacy of Florence Girard."*

School of Computing and Academic Studies (SoCAS)

Burnaby Campus (BBY), Downtown Campus (DTC)

- BCIT has joined the AMII AI Workforce Readiness project, enabling SMEs from BCIT to collaborate on AI-related open-source teaching modules with other SMEs from 27+ other post-secondary institutions across Canada. **Bahareh Shahabi, Communication Faculty-SoCAS**, helped initiate and is the BCIT liaison. A BCIT Workforce Readiness Curriculum Development Team has been established with internal calls for SMEs to identify AI-related pedagogy. BCIT has already had a proposal accepted on **AI in Healthcare**, a collaboration between School of Health Sciences faculty and School of Computing and Academic Studies faculty from the Communication Department, working alongside their counterparts from the University of British Columbia Okanagan, Bow Valley College, and MacEwan University. Faculty members from SoCAS and SoB&M have also submitted to the next rounds of calls for proposals, scheduled for 2026.

- **BCIT's leadership in cybersecurity education** was recognized by Maclean's Magazine: "Anyone interested in answering the five-alarm call for more cybersecurity professionals might look first to the British Columbia Institute of Technology, which has multiple paths into the field." Drawing on our specialized landing page of bcit.ca/studycybersecurity, the article outlined our wide range of offerings. 2025 data from the World Economic Forum shows that organizations worldwide consistently rank ransomware as one of their top concerns, and interest in closing the cybersecurity skills gap is high.

School of Construction and the Environment (SoCE)

Burnaby Campus (BBY)

- Female student enrolment in geospatial technologies is strong, with 40% of GIS program students being women.

- The school is building a replacement for its aging world-unique Ironworker Tower, a hands-on training facility for steel trades students. The new hybrid tower will feature steel, mass timber, and concrete, provide interdisciplinary, real-world construction experience and reflect current industry standards and materials.

- Mass Timber Training Hub:
  New Course Launch – Designing with Mass Timber - Principles of Sustainability in a two-week pilot from September 29 to October 10; 24 design professionals explored using bio-based materials from sustainably managed forests to create eco-friendly, high-performance buildings.

  Engaging Building Officials - Project Leads from the Mass Timber Training team were invited to facilitate sessions at yearly zone meetings for building officials from all regions of British Columbia. Over 250 building officials are expected to participate. The presentations

enable building officials to focus on and expand site considerations and help inspectors know what to look for on a MT project site.

Mass Timber Modular Education Hub Initiative - The Mass Timber Modular Learning Hub is a collaborative project led by BCIT and partners, creating a full-scale mass timber module on campus. This hands-on space serves as an educational and demonstration hub for students, industry professionals, and the public.

Advancing Off-Site Construction for SSMUH (Small Scale Multi Unit Housing) - Over 120 participants joined the Advancing Off-Site Construction for SSMUH webinar, exploring how off-site methods can address BC's housing needs. The session covered policies, design, and delivery for small-scale multi-unit housing, with more training planned for Winter 2026.

School of Energy (SoE)

Burnaby Campus (BBY)

- On October 29, thirty Electrical Engineering and Master of Engineering in Smart Grid Systems and Technologies students and instructors from BCIT visited BC Hydro's Ruskin Dam Generating Station in Mission, BC, touring the hydroelectric facility, learning about generating equipment and control systems. BC Hydro experts provided instruction and introduced the CPC Apprenticeship Program, inspiring many. Organized by the Electrical Engineering and Technology (EET) Department and BC Hydro's Communications, Protection & Control team, the trip linked classroom theory with real-world power generation.

  The visit deepened students' understanding of power engineering; one said, "nothing compares to standing on a running turbine and feeling the electricity in the air," while another expressed excitement about applying classroom concepts in their future careers.

School of Health (SoHS)

Burnaby Campus (BBY)

- The **Simulation Team** published a qualitative study in **SSH Simulation in Healthcare Journal** examining how debriefers give and receive feedback in simulation-based education. Engaging 27 faculty from various health fields, the study identified four main themes that enhance feedback: building trust, fostering growth mindsets, promoting psychological safety, and using structured frameworks like **DASH** and **PEARLS**. The results emphasize that relational and cultural practices are central to effective feedback and ongoing professional development. This work supports the SoHS Simulation Strategy and demonstrates the team's leadership in advancing simulation-based education at BCIT and beyond.

- **Brynn Tomie, Radiation Therapy Program**, launched an education podcast for BCIT students with BC Cancer guests. "BEAM ON" is a BCIT Radiation Therapy podcast where BCIT faculty, past and present students, and radiation therapists share personal clinical experiences with current and prospective students. The podcast allows students to engage with the information through story telling in a digestible and flexible manner. Listen to the podcast.

- **Cristina Scott, Cardiac Sciences Program**, presented ***"The Good, the Bad and the Ugly of ECGs"*** at the British Columbia Society of Laboratory Science (BCSLS) Symposium 2025.

School of Transportation (SoT)

Annacis Island Campus (AIC), Aerospace Technology Campus (ATC), Burnaby Campus (BBY), Marine Campus (BMC)

- On October 17, the **Heavy Mechanical Trades** division at AIC completed without any observations the annual Technical Safety BC audit of our industrial railyard facilities, equipment and training.

- The Heavy Mechanical Trades division met the growing demands from the transportation sector for upskilling technical training by delivering advanced hydraulics training to maintenance technicians from the **Global Container Terminals** in Delta (November 3 to 7).

- The Marine division successfully partnered with **Tricorp**, an indigenous lead development organization, to deliver a basic marine small vessel machinery operations course in Prince Rupert from November 17 to 28.

- The **Aircraft Structural Technician** apprenticeship began on November 3. Employees of aircraft manufacturers will attend our campus for one month each year for four years and there will be three intakes per year. This is the first apprenticeship program at ATC.

CATALYZE DIGITAL TRANSFORMATION

Financial Services

Burnaby Campus (BBY)

- Financial Services has implemented **Millennium Fast AR**, a third-party accounts receivable software, to enhance the efficiency and streamline the non-student invoicing process. This implementation addresses the limitations in Banner by improving processing times, supporting a higher standard of service to the community, and enabling more accurate and timely collections. This initiative represents a significant step forward in our ongoing commitment to strengthening interdepartmental collaboration and advancing process efficiencies.

Indigenous Initiatives & Partnerships

Burnaby Campus (BBY)

- The **CEDAR project** (Community Empowerment: Diversity and Authentic Reconciliation) has completed a series of videos of Indigenous people across Canada. They have been translated to French as required by the funder (Heritage Canada). The goal of the CEDAR recordings will form and enhance the online Indigenous Awareness Modules with the goal of providing authentic lived experiences, knowledge, real history, and a glimpse of the lives and cultures of Indigenous people coast to coast to coast.

School of Construction and the Environment (SoCE)
Burnaby Campus (BBY)

- **Quality Positioning Services** (QPS), which donated software to the **Geomatics department**, held on-campus training from September 15 to 18 for students and faculty on survey and navigation software, multibeam processing, and 4D geospatial analysis.

School of Energy (SoE)
Burnaby Campus (BBY)

- On November 4, Dr. Nipun Vats, Assistant Deputy Minister at ISED Canada, visited BCIT's BBY to observe the school's strengths in forensics, cybersecurity, and applied sciences. The tour included the Industrial Network Cybersecurity Lab, highlighting BCIT's practical training for future cybersecurity professionals. Dr. Vats commended BCIT's contributions to digital transformation and Canada's innovation ecosystem.

School of Transportation (SoT)
Annacis Island Campus (AIC), Aerospace Technology Campus (ATC), Burnaby Campus (BBY), Marine Campus (BMC)

- In September, the school received **GMDSS and ECDIS simulators** from Kongsberg Marine. Using cloud technology, these advanced tools provide realistic ship bridge training and improved benefits for instructors and students.

FOSTER VIBRANT COMMUNITIES

BCIT Alumni Association (the Association)

- The Alumni Relations Office has renewed valued partner contracts of the **Alumni Perks program** with Delta Hotels Burnaby, Vancouver Canucks, Abbotsford Canucks, and Executive Hotels & Resorts. These exclusive benefits promote alumni connection, support local businesses, and foster pride and long-term loyalty within the BCIT community.

- The Association held the first **BCIT Advantage Fair** on September 17 at BBY, featuring Alumni Perks Partners and companies such as Mark's Commercial, BC Lions, IKEA, BMO, and others offering discounts to the BCIT community. The event drew over 1,500 attendees, distributed prizes, and generated nearly $8,000 for student and alumni programs.

- The Association welcomed **999 new alumni** with a new grad email sent on October 10 detailing the upcoming events and benefits available to them.

- The winter e-newsletter was sent to **102,576** alumni on November 3, with stories including the Celebration of Impact and upcoming events.

- The Association has hosted and sponsored a total of **37 events since April 1** offering funding and resources to enhance student and alumni engagement with school and student partners.

Applied Research - Centre for Applied Research and Innovation (CARI)

- BCIT launched the new BCIT Applied Research Showcase series highlighting and exploring the real-world research and innovation taking place across all BCIT schools and at CARI.

- CARI welcomed members of the BC Society of Engineering and Geoscience (BCSEG) for a presentation and tour of our research facilities, led by MAKE+ Researcher and BCSEG Richmond Delta Branch member Fardin Barekat, P.Eng. The event connected engineering and geoscience professionals with BCIT's research community and showcased the resources and expertise available through CARI.

- BCIT researchers Joey Dabell, Project Leader with the Smart Microgrid Applied Research Team (SMART) and Yvette Jones, Project Leader with the MAKE+ applied research group are collaborating to identify what works, and what doesn't, for people with diverse accessibility and mobility needs when charging an EV in public spaces. The team is helping to lay the groundwork for Canada's first national accessibility guideline and eventual standard for electric vehicle charging infrastructure.

- **Dr. Alejandro Adem, President NSERC** (National Sciences and Engineering Research Council of Canada), toured CARI's labs and met with Anika Singh, PhD, Dr. Michael Chan of the Natural Health & Food Products Research Group, and Dr. Jaimie Borisoff, Director of MAKE+, to learn about NSERC supported research in health, nutrition, and accessibility technologies.

- CARI joined the **2025 Hardware Unconference**, where innovators, startups, and researchers explored hardware, robotics, and product development. BCIT's MAKE+ group hosted the Solutions Lounge, featuring projects like the BEAST wheelchair, quadruped robots, and reverse engineering demos. The event strengthened industry ties, student involvement, and collaboration among BCIT's research labs.

Government Relations

- **Campus Connection Week** took place on October 14 to 17 and **MP Wade Chang** toured BBY to learn more about BCIT's programs and **MP Jonathan Wilkinson** visited BMC.

- **MLA Lawrence Mok**, Official Opposition Critic for Skills Training and International Credentials, visited BBY on October 24. MLA Mok's visit focused on health and construction training, student outcomes, and changes in international student policy.

- **MLA Paul Choi,** Parliamentary Secretary for Trade, visited BBY on November 5 to discuss business programs, trade, and global partnerships.

Institute Sustainability

- The BCIT Library celebrated **Climate Action Week 2025** from November 1 to 7, joining other libraries across BC. The event promoted reflection and action for sustainability with activities such as a plant swap, climate book club, and challenge games at BBY.

Library Services

- From September 1 to October 31, **Library Services** saw high engagement, supporting **4,537 students** through tours, events, and class visits. **Tutoring services** in the Learning Commons began September 17 and assisted **626** students, while WriteAway handled 56 submissions since launching September 15. **Learning Skills** support aided **116** students via meetings and drop-ins. The Learning Commons held **54** events, seminars, or class visits, drawing **3,350 attendees**.

- Other library events, including a book club, three **Storytime sessions**, and five **Food for Thought talks**, engaged 237 participants. The Food for Thought series, in partnership with LTC, drew 175 in-person attendees and 125 online viewers. This program has enhanced faculty collaboration, reflective teaching practice, and cross-departmental connections, supporting ongoing professional growth and learning.

- **MEDIAWORKS** experienced significant activity during this period. A total of **950 participants** attended 56 tours, while regular visits reached **4,635**. MEDIAWORKS fulfilled 94 project requests, providing hands-on assistance with creative, technical, and multimedia work. These results highlight MEDIAWORKS' continued contribution to experiential learning and project-based collaboration across campus.

- The library maintained high engagement during the fall term, with **627,083** electronic titles available and **68,757** online views. Librarians handled **3,743** queries and processed **1,180** interlibrary loan requests. In-person visits at BBY totaled **44,383**. These figures highlight strong participation in both digital and physical library services at BCIT.

School of Computing and Academic Studies (SoCAS)

Burnaby Campus (BBY), Downtown Campus (DTC)

- **From student to cybersecurity leader: Award-winning alum Anthony Green** has built an impressive career while mentoring others and giving back to the tech community. His story shows how curiosity, hands-on learning, and lifelong growth can open doors to incredible opportunities in cybersecurity. He told us: *"AI isn't going to replace people, it's going to replace people who don't know how to use it."*

- **Computing students organized a hackathon** at BBY on November 7 to 9, drawing over 100 participants. It was sponsored by the Computing Department, BCIT Student Association, and BCIT Alumni Association. HTTP Hacks 2025 required solid software development skills of participants, no vibe coding allowed! Students created apps ranging from a waste bin fullness monitor to financial stock analysis and comparison. See the project gallery.

- Over 120 students from a range of high schools participated in the BC Youth Developer Collective (BCYDC) Daydream Hackathon at DTC, in the TEC Hub. Hosted by the Computing Department, the participants were thrilled with their experience: new coding skills, new friends, new projects. BCYDC is **British Columbia's Largest High School Developer Community**.

- The Front-End Web Developer (FWD) fast-track Certificate Program hosted a **WordPress + FWD** meeting at DTC in October. Over 40 members of the local web development community met in the Tech Collider to talk about their international industry experiences and provide insight for current students.

School of Construction and the Environment (SoCE)

Burnaby Campus (BBY)

- SoCE Forestry students Heather Clark and Tanya Steinauer received the Future Faces of Forestry award at the 2025 BC First Nations Forestry Conference. Supported by the Indigenous Forestry Scholarship, they gained valuable industry experience and connections, with internships at BC Ministry of Forests and BC Timber Sales.

- In the fall, ConnectHER Hub promotes inclusion in trades through mental health, equity, and networking events. Monthly lunches link women, gender-diverse students, alumni, and allies to resources and peer support.

- Burnaby **MLA Anne Kang** attended the **United Way pancake breakfast** on October 31, supporting BCIT staff and students in fundraising efforts. The 2025 SoCE United Way Pancake Breakfast successfully raised $9,533.75, demonstrating strong community engagement and support for the cause. 2025 BCIT United Way Pancake Breakfast | Flickr

School of Transportation (SoT)

Annacis Island Campus (AIC), Aerospace Technology Campus (ATC), Burnaby Campus (BBY), Marine Campus (BMC)

- The school teamed up with **UBC Geering Up** and hosted a five-day hands-on summer camp at ATC. UBC Geering up is a STEM (Science, Technology, Engineering, Mathematics) camp for elementary and high school students to investigate these subject matters in a safe learning environment. Students built a glider model, used flight simulators, simulated air traffic control, assembled circuit boards, learned about turbine engines, and listened to live YVR air traffic control from the observation deck. This successful event is planned for next year.

- On September 25, Steve Grone (AIC Heavy Duty Instructor) and **Richard Haire** (Business Development Manager) spoke at Fleet Forward Metro Vancouver, targeting organizations with medium and heavy-duty fleets. They introduced the upcoming Zero Emissions Vehicle (ZEV) Safety course for these vehicles, launching early next year, which prepares Red Seal technicians to safely service electric vehicles with high-voltage systems.

- On November 6, Debbie Power (Program Coordinator) attended the **Musqueam Career and Trades Exploration** event in Vancouver. She shared marine training and career pathway information and developed connections with Musqueam Nation staff.

Student Success

- **Medical Training Collaboration** - BCIT will host a PGY-6 Adolescent Psychiatry Fellow from UBC for a 4-to-6-week clinical rotation starting January 2026. This enhances BCIT's profile as an elective site for trainees from UBC, SFU, and nationwide, potentially

decreasing student mental health wait times. GPs and counsellors can make extra referrals during this period.

- **Nursing Services Innovation** - To accommodate the rigorous schedules of Health Sciences students, the nursing team administers mass vaccination clinics in NE04, thereby providing accessible essential health services that align with academic requirements.

- **Overdose Prevention and Harm Reduction** - Introduced an Overdose Prevention & Response Plan following provincial guidelines, covering naloxone training, stigma reduction, and harm reduction education. Distributed 485 naloxone kits and 259 fentanyl test strips to over 900 participants via outreach and workshops. Launched an amnesty policy for housing students to promote help-seeking. Continually working with BCITSA and community partners to enhance awareness and response efforts.

- **Student Wellbeing Action Plan Rollout** - Continued the Student Wellbeing Action Plan with a focus on mental health literacy, early intervention, and coordinated care. Updated distress response guides, trained faculty/staff, and expanded culturally relevant partnerships. Embedded wellbeing priorities in policy and campus engagement.

- **Student Housing Expansion** - Tall Timber Student Housing opened in September, offering emergency units and an expanded Residence Life team. Emergency housing is available within 48 hours of a request.

ENRICH PARTNER EXPERIENCES

Applied Research - Centre for Applied Research and Innovation (CARI)

- On July 29, Dr. Paula Brown, Director of BCIT's Natural Health and Food Products Research Group (NRG), joined U.S. health officials in Washington, DC to announce new rules to protect US citizens from dangerous synthetic drugs misbranded as kratom.

- Dr. Mona Nemer, Canada's Chief Science Advisor, visited CARI, along with Vanessa Sung, PhD, Policy Advisor with the Office of the Chief Science Advisor.

- BCIT will partnering with Melanie Mark, Former Minister of Advanced Education and Skills Training, and her business Remarkable First Nations Regenerative Industries on an important and exciting project to recycle EV batteries. This initiative is a collaborative effort across BCIT, bringing together the Smart Microgrid Applied Research Team, the SoE, BCIT MAKE+, and the SoT.

BCIT Foundation

Burnaby Campus (BBY)

- The **2025 Winter Appeal** runs from November 18 to December 31, targeting alumni and campus giving. This year, the Foundation and BCIT's Student Life team are raising funds

for the new Student Wellbeing Action Fund, which supports students facing food and housing insecurity so they can focus on their studies and career goals.

- On October 23, the Foundation hosted its first **Celebration of Impact event**, welcoming over 100 guests including award recipients, donors, alumni, and past presidents. Dr. Jeff Zabudsky interviewed students who discussed overcoming challenges, juggling studies with financial and personal responsibilities, and expressed gratitude for donor-funded awards.

- On November 12, the **INSPIRE Campaign Celebration** was held to mark the end of fundraising with a private event for 60 key supporters, including BCIT Foundation members, Board members, executives, and deans.

- BCIT has been awarded a $1.5M private donation to establish **the Welding Pavilion**, a sheltered facility for welding students. Construction is underway, with the slab pour phase completed, and the project is scheduled for completion by November 25. Contingent upon the donor's availability, the unveiling ceremony will be coordinated with SoCE and planned for the new year.

- **The Robert Bosa Carpentry Pavilion**, named after Bosa Properties' $4M pledge to BCIT in 2021, will feature a two-story mass timber workspace built to LEED Gold and Net Zero Ready standards. Groundbreaking for this pavilion and the Marine and Mass Timber Pavilion at BBY is expected in early January 2026, pending Ministry approval.

Indigenous Initiatives & Partnerships

- **Bachelor of Science in Nursing Connect** seeks to extend the BCIT nursing program to remote and Indigenous communities using cloud technology, following a Health Sciences Centre tour and a productive discussion with the P.A. Woodward Foundation.

Institute Sustainability

- The **BCIT Centre for Ecocities** launched two online tools that help BC communities take climate action. The Consumption-based Solutions for Climate Action Guide and the CBEI and EF Archetype Tool for BC Communities are designed to help local governments, businesses, and communities adopt practical strategies to reduce pollution, shrink ecological footprints, and promote equity and community wellbeing. Five students from BCIT's Computer Systems Technology Diploma program created the web interface for the archetype tool. A launch webinar for the tools was held in June for BC local government leaders and climate practitioners. This project was supported by the Real Estate Foundation of BC.

- BCIT **celebrated World Rivers Day** on September 25 with a tour of Guichon Creek led by BCIT Honorary Doctorate, Mark Angelo. The event highlighted restoration work by the BCIT Grounds Team and Renewable Resources students, while nearby booths featured information from BCIT's Green Team, SoCE, Institute Sustainability, Campus Planning, Facilities, and partner organizations.

School of Computing and Academic Studies (SoCAS)

Burnaby Campus (BBY), Downtown Campus (DTC)

- The technology sector is experiencing layoffs, fewer entry-level jobs, and uncertain AI effects, with growth mainly in AI, cloud computing, cybersecurity, fintech, and green tech. BCIT Computing has cut its January diploma intakes to align with student interest and industry needs and is refocusing efforts to adapt to these trends.

- The MSc in Applied Computing launched its internship and R&D page, leading up to availability of **applied computing interns in spring 2026**. Faculty have already secured several internships for this first group of Masters students.

- BCIT highlighted its expertise as part of Cybersecurity Awareness Month in October. **Digital Forensics and Cybersecurity faculty Dr. Maryam Raiyat Aliabadi** was on Global News and CTV to discuss the importance of cybersecurity education for children. We also updated and released the Cybersecurity Education at BCIT video. And current student **Mohammed Jowarki** joined CTV news to discuss his project on AI-generated phishing scams. He told CTV about the growing trend of bad actors using AI tools to create thousands of highly realistic phishing emails within seconds.

School of Construction and the Environment (SoCE)

Burnaby Campus (BBY)

- **Steve Finn,** AD Natural Resources, represented British Columbia at the **Canadian Forestry Accreditation Board meeting**. By reviewing forestry programs across the country, he seeks to introduce best practices and fresh innovations to BCIT's Forest and Natural Areas Management program, ensuring it upholds leading professional standards.

- **Shawna Waberi**, program head of BCIT Mining, contributed *"A Collaborative Approach to the Mining Talent Challenge: Perspective of a Mining Educator"* in Issue No.1 of the **2025 BC Mining Review digital magazine**.

School of Transportation (SoT)

Annacis Island Campus (AIC), Aerospace Technology Campus (ATC), Burnaby Campus (BBY), Marine Campus (BMC)

- On September 27, BMC presented its fast rescue boat simulators at **Port Day** at Canada Place in Vancouver. The event allowed interaction with the public, informed potential students about marine careers, and fostered relationships with marine organizations.

- On October 16, **Richard Haire**, Business Development Manager, attended the **National Marine Workforce Development Strategy Conference** in Toronto, ON. The event focused on strategies to recruit and retain mariners, navy cadets, and navy reservists, bringing together representatives from academia, government, the Royal Canadian Navy, the Canadian Coast Guard, and other public sector organizations. The event ended with a reception aboard one of the Navy's newest ships - HMCS Margaret Brooke.

- **Julie Raymond (Assistant Director, Innovation & Research, Institute maritime du Québec) visited BMC** on October 24. She visited to discuss joint projects and funding, strengthening inter-campus collaboration and creating new partnership opportunities.

- Monetized the industrial railway assets at AIC by hosting a movie production three-day operation (November 13 to 15).

INFORMATION NOTE
March 31, 2025

PREPARED FOR: Board of Governors

PREPARED BY: Raimonda De Zen, Director, Enterprise Risk and Internal Audit

ISSUE: Public Interest Disclosure and Protection Annual Report (FY 2024/25)

OBJECTIVES:

To provide the Audit and Finance Committee with an annual summary report on matters that have been brought forward as suspected wrongdoing and reported to BCIT's designated officers under Public Interest Disclosure and Protection - Policy #1100.

BACKGROUND:

In April 2024, BCIT's Public Interest Disclosure and Protection - Policy #1100 and associated procedures #1100-PR1 came into effect. This policy was created with the intent to align BCIT to the Public Interest Disclosure Act (PIDA). Policy #1100 outlines the types of suspected wrongdoing that can be brought forward by a BCIT employee and that will be examined according to the parameters set within the policy and procedures.

As BCIT must abide by PIDA, one of the mandatory requirements under PIDA is that BCIT must report annually on the reports of wrongdoing and investigations. The reporting is for information purposes only and will not disclose the identify of the disclosers, the respondents, and/or the witnesses, nor will it identify the nature of the suspected wrongdoings brought forward. This restriction is in alignment with PIDA requirements.

This report covers the period of April 1, 2024 - March 31, 2025, which also aligns with the first year of Policy #1100's existence.

The following table captures statistical information related to any reports received by the designated officers during the period noted above. It does not contain any statistics relating to reports and/or investigations that were already underway from the prior fiscal year and that was completed during fiscal 2024/2025.

Summary Information Relating to Disclosures	Fiscal 2024/2025 (Quantity)	Notes
Total number of disclosure reports received	1	
Total number of disclosure reports reviewed	1	The suspected wrongdoings raised by the disclosers did not fit within the parameters of suspected wrongdoing as outlined by BCIT's Policy #1100. The disclosers were informed, and no further analysis or investigation was undertaken.
Total number of disclosure reports indicating wrongdoing substantiated	Nil	

Disclosers have the option to provide their reports directly to the designated officers, to their supervisor who convey their disclosure report, and/or may use a confidential email inbox (i.e. confidential_line@bcit.ca) which is accessible by the designated officers only.

Board of Governors Open Meeting – December 3, 2025
4.0 Board Chair's Comments - Verbal
5.0 President's Comments - Verbal

INFORMATION NOTE
December 2, 2025

PREPARED FOR: Board of Governors

PREPARED BY: Jeff Zabudsky, President

ISSUE: President's Activities

Reporting to the Board of Governors, highlights of the President's activities from October 7 to December 2, 2025. While this document highlights activities that Jeff Zabudsky took part in, some of the activities are also referenced in more detail in the Institute Report located elsewhere in the Board package.

October 8, 2025

- Meeting with Sector Board Chairs and Heads in the province (Research Universities Council of British Columbia; Pacific Association of Canadian Institutes and Universities; and BC Colleges).
- Post-Secondary Sector Association Chairs and Heads meeting.
- 2025 Fall Big Info event at Burnaby campus.

October 9, 2025
Convocation ceremony at Simon Fraser University.

October 10, 2025
Hosted a visit of senior executives from ICBC, including interim CEO, Jason McDaniel.

October 15, 2025
Greater Vancouver Board of Trade lunch address with UBC president, Dr. Benoit-Antoine Bacon.

October 16, 2025
Hosted a visit to the Marine Campus from MP Jonathan Wilkinson as part of Colleges and Institutes Canada Connection Week. It is a national outreach and engagement campaign that brought Members of Parliament and Senators to post-secondary campuses across the country.

October 17, 2025
Virtual meeting with Neil Lilley, a consultant charged with leading the strategic planning review at the Post-Secondary Employers' Association.

October 20, 2025
A reception hosted by the Consulate General of Germany in honour of their Unity Day national holiday.

October 21, 2025

- Governance Committee meeting of the BC Council for International Education.
- Briefing to presidents of the Pacific Association of Canadian Institutes and Universities (formerly BCAIU) from Global Public Affairs, a government relations firm.

October 22, 2025

- Lunch with the President for a small group of BCIT employees.
- Virtual meeting with PSFS Deputy Minister Trevor Hughes and Assistant Deputy Minister, Kim Horn.

October 23, 2025

- Greater Vancouver Board of Trade event “Mining For a Resilient and Productive Economy: Strengthening Canada’s Future”.
- BCIT Foundation and Alumni Association inaugural “Celebration of Impact” event, which brought together award donors, student award recipients, past association presidents, and alumni.

October 24, 2025

- Hosted a visit to the Burnaby campus from provincial MLA Lawrence Mok, official opposition critic for skills training and international credentials.
- Attended the president’s installation ceremony for Dr. James Mandigo at the University of the Fraser Valley.

October 26-31, 2025

Travel to Ottawa for meeting and events, including:

- October 27
  - BC Post-Secondary Reception organized on behalf of the Research Universities’ Council of British Columbia (RUCBC), Pacific Association of Canadian Institutes and Universities (PACIU) and BC Colleges with senior post-secondary and federal government leaders in attendance.
- October 29
  - Meeting organized by Universities Canada and Regional and Provincial Associations for Board Chairs and Executive Directors
  - Polytechnics Canada National Strategy Group meetings, which is a series of annual consultative meetings held with senior federal government officials. Each member institution also invites a business partner to join the event – this year’s BCIT invitee was Scott Comfort, president, Seagate Mass Timber.
  - Polytechnics Canada National Strategy Group reception for a larger group of elected and unelected officials as well as sector representatives and business partners.
- October 30
  - Polytechnics Canada National Strategy Group meetings continued (without business partners)
  - Polytechnics Canada board meeting.
- October 31
  - Greater Vancouver Board of Trade Annual General Meeting and subsequent Board of Directors meeting.
  - BC Council for International Education board meeting

November 3, 2025

Attended the annual Webster Awards dinner ceremony as guest of the BCIT School of Business + Media.

November 4, 2025

- Greater Vancouver Board of Trade event “Metro Vancouver - Together We Make Our Region Strong” with speaker Burnaby Mayor, Mike Hurley.
- Visit to Burnaby campus from Nipun Vats, Assistant Deputy Minister, Science and Research, Innovation, Science and Economic Development Canada, and Tina Barton, Regional Economic Advisor, Pacific Region
- Meeting with Mark Angelo, inaugural chair, BCIT Rivers Institute, former head of BCIT's Fish, Wildlife and Recreation Program, and recipient of a BCIT honorary doctorate.

November 5, 2025

- Board meeting, Pacific Association of Canadian Institutes and Universities.
- Vancouver General Hospital 50th anniversary reception of the Biomedical Engineering Department. Many BCIT graduates have been employed there over the years.
- Ajay Patel, president, Vancouver Community College.
- Reception in honour of Ryan Beedie, recipient of a National Citizen Award from the United Nations Association in Canada.

November 6, 2025

BCIT 2025 Long Service Awards Celebration for employees who have worked at the Institute for more than 20 years.

November 12, 2025

- Executive meeting of the Skilled Trades Training Council of BC.
- Meeting of the Skilled Trades Training Council presidents with Hon. Jessie Sunner, Minister, Post-Secondary Education and Future Skills.
- Meeting with Alan Schroeder, Director of International Education, Ministry of Education and Child Care
- BCIT Inspire Celebration, an event to mark the closing of the INSPIRE fundraising campaign.

November 13, 2025

- Meeting with representatives from the provincial Ministry of Jobs, Economic Development and Innovation regarding the government’s Industrial Strategy titled “Look West”, which was subsequently released on November 17.
- Virtual meeting with Christina Zacharuk, Research Universities Council of British Columbia.

November 19, 2025

President’s Connect meeting with senior management leaders at BCIT.

November 21, 2025

Meeting for post-secondary leaders with Hon. Jessie Sunner, Minister of Post-Secondary Education and Future Skills and Deputy Minister, Trevor Hughes regarding sector sustainability.

November 25, 2025

- BCIT Foundation Board meeting.
- Business + Higher Education Roundtable meeting regarding their Strategic Summit held on September 22.

November 26, 2025
Executive meeting of the Skilled Trades Training Council of British Columbia.

November 27, 2025
BCIT Burnaby Campus tour for Don Lindsay, former CEO, Teck Resources.

November 28, 2025

- Meeting with provincial post-secondary sector Board Chairs and Heads.
- Virtual meeting with Christina Zacharuk, CEO, Research Universities Council of British Columbia.
- Meeting with Jodi Evans, Managing Partner, and Troy Kay, Partner, Deloitte Canada Vancouver office.

December 1, 2025
BCIT President's Forum for all employees.

DECISION NOTE
November 20, 2025

PREPARED FOR: Board of Governors

PREPARED BY: Navida Suleman, CFO and VP, Administration
Sunny Jassal, CISO

ISSUE: Acceptable Use of Information Technology – Policy #3501, and Information Security – Policy #3502

APPENDICES:

1. Appendix A: Acceptable Use of Information Technology - Policy #3501, draft
2. Appendix B: Acceptable Use of Information Technology - Policy #3501, redline
3. Appendix C: Information Security Policy – Policy #3502, draft
4. Appendix D: Information Security Policy – Policy #3502, redline
5. Appendix E: Information Security Procedure – Procedure #3502, current (in Aprio)

RECOMMENDATION:

THAT the Board of Governors approves revisions to the *Acceptable Use of Information Technology - Policy #3501, and the Information Security – Policy #3502*, and the retirement of the Information *Security Procedure – Procedure #3502*.

SUMMARY:

On November 18, 2025, the Audit and Finance Committee reviewed and recommended Board approval of two revised policies and the retirement of the procedure. The policies underwent their scheduled five-year review to uphold BCIT's cybersecurity and IT risk standards. The review forms part of BCIT's commitment to maintaining and improving its cybersecurity and information technology risks. The Chief Information Security Office (CISO) undertook a comprehensive review of existing language and policy design. The proposed revisions include several added definitions and increased readability. The revised Policy #3502 renders its related Procedure #3502 obsolete; therefore, the retirement of Procedure #3502 is also recommended currently.

The policies are aligned with advanced cybersecurity frameworks e.g., National Institute of Standards & Technology Cybersecurity Framework [NIST CSF], ISO 27001, Zero trust). The Framework emphasizes clarity and focused, actionable controls.

The draft revised policies were reviewed by the CISO Office in consultation with IT Services Management and various risk functions - BCIT's Risk Advisory Committee (including representatives from Information Access & Privacy; People, Culture, and Inclusion; Safety, Security and Emergency Management; Enterprise Risk Management) and by the Policy Management Office.

The draft policies were subject to an extended 45-day community review, and feedback was incorporated into the final drafts. In addition, on the recommendation of BCIT's Policy Review Committee, an optional legal review was undertaken for Policy #3501 to ensure alignment with privacy and FOIPPA legislation. The policy includes feedback from that legal review.

ACCEPTABLE USE OF INFORMATION TECHNOLOGY – POLICY #3501

REVISED DRAFT

BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

Acceptable Use of Information Technology [DRAFT]

Policy No:	3501
Version:	7
Category:	Information Management
Approval Body:	Board of Governors
Executive Sponsors:	VP Finance & Administration; VP People, Culture, & Inclusion
Department Responsible:	Cyber Security Office
Directory of Records Class:	0650-15
Approval Date:	Pending

Policy Statement

This policy outlines the responsibilities of members of the BCIT community with respect to the responsible and acceptable use and security of BCIT IT Resources, which include technology, data, digital assets, systems, equipment and devices. It sets out requirements for the responsible, ethical, and legally compliant use of technology resources in support of BCIT operations, teaching, research, and administrative activities.

Through this Policy, BCIT seeks to foster a secure, innovative, and collaborative digital environment supporting BCIT's teaching, learning, research, and administrative goals. This Policy incorporates and adopts a risk-based and collaborative approach, encouraging both responsible technology use and the promotion of innovation to advance BCIT's academic mission. BCIT affirms its commitment to the principles of academic freedom.

Purpose of Policy

The purpose of this Policy is to establish clear expectations and requirements for the responsible and acceptable use of BCIT IT Resources by all users.

Who This Policy Applies To

This Policy applies to all individuals who use BCIT IT Resources, including staff, faculty, students, contractors, third-party contractors, researchers, and visitors. It also applies to users who use Personal Devices in connection with BCIT IT Resources.

Consequences of Policy Violation

Compliance with this Policy is mandatory for all users of BCIT's IT Resources. Users who breach this Policy or engage in Misuse will be subject to discipline, up to and inclusive of dismissal or expulsion.

BCIT reserves the right to restrict, suspend, or withdraw access to BCIT systems and services, including computing privileges and network connectivity.

Investigations of suspected Misuse and any resulting actions will follow established Institute procedures and principles of fairness and due process.

In cases where Misuse or other user equipment or activity poses an immediate security or operational risk, BCIT may take temporary measures to protect Institute systems, such as disconnecting or quarantining affected devices, until the issue is investigated and resolved.

Person Device connecting to BCIT networks may also be subject to reasonable security restrictions to protect Institute systems and data integrity.

Duties and Responsibilities

Role	Responsibilities
Board of Governors and BCIT Executive	The BCIT Board of Governors and the BCIT Executive actively support and promote the acceptable use of information technology.
Chief Information Security Officer (CISO)	The CISO provides leadership and oversight for the security of BCIT's IT systems, data, and digital assets. Their responsibilities include developing and enforcing security policies and standards, ensuring compliance with applicable regulations, and maintaining a secure and resilient infrastructure capable of detecting, preventing, and responding to cyber threats. The CISO also serves as the final authority for approving security exceptions.
BCIT Management	Members of BCIT Management are responsible for ensuring that staff and others under their supervision are aware of their responsibilities for the acceptable use of information technology.
Instructors and Teaching Faculty	Instructors and Teaching Faculty are responsible for ensuring that students under their supervision are aware of their responsibilities for the acceptable use of information technology.
IT Administrators	IT Administrators and other privileged Users must protect the security of BCIT It Resources and must not abuse their elevated privileges.
Safety, Security and Emergency Management	The Safety and Security and Emergency Management department is responsible for monitoring BCIT's physical environment to ensure Misuse and other unacceptable behaviour is minimized.
Risk Management	The Enterprise Risk Management group is responsible for monitoring liability risk associated with the use and Misuse of BCIT IT Resources.
Users	All Users are responsible for familiarizing themselves with their responsibilities under this Policy. Users should promptly report known or suspected instances of Misuse.

1. General Accountability

All use of BCIT IT Resources is subject to compliance with this Policy. It is the responsibility of all users to ensure they are familiar with and comply with this Policy.

2. Access

BCIT's IT Resources may be accessed and used only by members of the BCIT community who are granted access privileges by BCIT. All access and use are subject to compliance with this Policy, other applicable BCIT Policies, including Policy 3502 Cyber Security, and with the applicable laws of British

Columbia and Canada, including the *Criminal Code,* the *Copyright Act,* the *Human Rights Code* and FIPPA.

3. Copyright and Intellectual Property

When using BCIT IT Resources, users must comply with all applicable laws and Institute policies related to intellectual property and copyright, including BCIT Policy 7505, Use of Material Protected by Copyright, including by refraining from any acts that infringe upon copyright in relation to computer programs, data collection, work product, and any literary, dramatic, artistic and musical work.

4. Usage and Monitoring

BCIT monitors the use of its IT Resources for operational, security, and compliance purposes. Monitoring supports the protection of BCIT Data, detection and response to cyber security threats, and compliance with legal, policy and regulatory obligations. Users should understand that this monitoring and maintenance may involve access to Personal Use Records or Personal Information of users.

i. BCIT makes reasonable efforts to ensure monitoring activities are limited to what is necessary and proportionate to achieve the above purposes and are conducted in compliance with applicable legislation, including FIPPA.
ii. Users should be aware that information created, transmitted, or stored using BCIT IT Resources may be subject to access or review under circumstances such as:
    a. a suspected or confirmed security or policy incident;
    b. an investigation under Institute, legislative, policy or legal authority; or,
    c. routine system performance or security assurance activities.
iii. BCIT will not intentionally access, use or disclose Personal Information or personal records stored on BCIT IT Resources without the user's knowledge and consent unless:
    a. authorized or required by law,
    b. where securing the user's consent would compromise the health and safety of any individual or group; or,
    c. where the information is needed for an investigation or proceeding related to a breach of law, policy or employment duties and seeking consent would compromise the availability of required information or the investigation or proceeding.
iv. BCIT also reserves the right to access information or communications stored on BCIT IT Resources where needed to transition employment responsibilities after an employee departs from their employment or is on an extended leave.
v. Access requests involving intentional access to a user's Personal Information or Personal Use Records stored on BCIT IT Resources must be pre-authorized by the Chief Information Security Officer or their designate. Where applicable, such access will also be subject to oversight and approval from the Information Access and Privacy Office and/or the Human Resources department to ensure compliance with privacy, legal, and organizational requirements.

vi. BCIT recognizes the importance of privacy, academic freedom, and the confidentiality of research data. Routine monitoring of IT Resources does not involve intentional access to research data, academic work, or personal communications except as described in this Policy.
vii. Personal Devices are not subject to routine monitoring. However, network activity from Personal Devices connected to BCIT systems may be logged to detect anomalies, threats, or policy violations.
viii. All monitoring and logging activities are recorded, audited, and subject to appropriate oversight and accountability.

5. Connecting Equipment to the BCIT Network

Users are subject to the following requirements regarding devices and equipment:

i. BCIT-owned and managed equipment, including desktops, laptops, mobile devices, servers, and network-enabled systems, must comply with Policy 3502, Cyber Security and cyber security standards and requirements. These devices are centrally managed and monitored by IT Services to ensure appropriate patching, antivirus protection, and security configurations.
ii. The use of Personal Devices is permissible to enhance learning, teaching, and productivity, provided that such use does not create risks to the security, privacy, and integrity of BCIT IT Resources. BCIT reserves the right to restrict or impose conditions or security controls on the use of Personal Devices where necessary to protect BCIT IT Resources.
iii. Recognizing that academic programs and research projects often involve testing or deploying specialized technologies, faculty and research teams may connect experimental or instructional devices (including IoT or prototype systems) to approved lab or research networks. Such connections must be coordinated with the Cyber Security Office to ensure that security controls and network configurations protect both the research environment and the broader campus network.
iv. Internet of Things (IoT) devices (e.g., smart TVs, sensors) intended for use in buildings and in research or academic labs must be registered and approved by IT Services prior to connection. IoT devices used solely for instructional or research purposes may be connected to isolated or sandbox environments with appropriate safeguards and faculty oversight.
v. To maintain a secure and reliable technology environment, BCIT may implement reasonable measures to safeguard network performance, data integrity, and BCIT systems. These measures may include monitoring, restricting, or temporarily disconnecting devices—whether BCIT-owned, personal, or research-related—if they are determined to pose a security or operational risk to BCIT.

6. Use of BCIT Information on Non-BCIT Equipment

BCIT recognizes that users may need to access BCIT enterprise systems or communication tools from Personal Devices such as smartphones, tablets, and laptops. To protect BCIT Data while maintaining flexibility, Personal Device use is permitted under the following conditions:

i. Devices must be protected by secure login and comply with any applicable BCIT access control policies.

ii. Devices must use current operating system updates, and full-disk encryption.
iii. Users must not store or transmit sensitive Personal Information or Confidential Information on Personal Devices unless explicitly authorized by their supervisor, and in such circumstances, data must be encrypted.
iv. Personal Devices on which BCIT Confidential Information or Personal Information is stored may not be removed from Canada unless such data has been securely and permanently wiped from the device or it is otherwise permitted under this Policy.
v. BCIT files must not be synchronized to unmanaged or personal cloud storage applications.
vi. Users must not disable, bypass, or circumvent BCIT security controls, including MFA prompts or device compliance checks.
vii. BCIT Data must be securely deleted from Personal Devices once no longer needed.
viii. Any lost, stolen, or compromised Personal Devices used for BCIT purposes must be reported immediately to IT Services or the Cyber Security Office.
ix. BCIT reserves the right to restrict or revoke access if a personal device poses a security or compliance risk to BCIT systems or data.
x. Users of Personal Devices maintaining or storing BCIT records or information may be required, upon request, to provide copies of all such records to BCIT and/or to securely delete them from Personal Devices.

7. Personal Information Collection and Use

The collection, use, storage, and transmission of Personal Information is governed by Policy 6700, Freedom of Information and Protection of Privacy, and Policy 3502, Cyber Security. In accordance with FIPPA, Users are required to complete a Privacy and Security Threshold Assessment (PSTA) before implementing new initiatives, systems, programs or projects that involve the use or processing of Personal Information.

8. Responsible Use of Software and Digital Tools

BCIT supports innovation in the use of digital tools and resources. Users may explore and use digital tools to enhance academic, research, and administrative activities. Software and applications that process, store, or transmit BCIT Data must comply with BCIT's security standards and licensing requirements, and be used in accordance with Policy 3502, Cyber Security.

i. BCIT supports the responsible use of open-source, open-educational, and cloud-based tools, provided they comply with BCIT's security standards, licensing requirements, and with Policy 3502, Cyber Security and Policy 5900, Educational Technology.
ii. Users must consult IT Services or the Cyber Security Office before adopting new digital tools for teaching or research that may involve the use of BCIT enterprise systems, cloud, or data, including where they involve the collection, use or disclosure of Personal Information BCIT employees or students.
iii. Downloading or installing unverified or unlicensed software to IT Resources is prohibited due to potential risks to security, compliance, privacy, and data integrity.

9. Responsible Use of Hardware Assets

Users are responsible for their own use of devices and equipment in compliance with this Policy, other applicable BCIT policies, and applicable laws. In addition, where applicable users must comply with the following requirements.

i. All users are required to use BCIT-owned IT assets securely, ethically, and in alignment with authorized academic, research, administrative, or operational activities, in compliance with BCIT policies, legal requirements, and cyber security best practices.
ii. BCIT-owned equipment (e.g., laptops, mobile devices, external drives) may be used off-campus by authorized users, provided appropriate security measures are in place to protect BCIT Data and assets. Users must take reasonable steps to prevent unauthorized access, loss, theft or Misuse of devices, including secure handling, storage, and prompt reporting of any incidents of loss, theft or device compromise.
iii. BCIT equipment remains the property of BCIT and must be returned upon request or at the end of employment, contract, or academic term.
iv. Personal Devices must not be used in ways that jeopardize the security or integrity of BCIT Data or BCIT IT Resources.
v. Users are prohibited from unauthorized modification, tampering, or Misuse of BCIT owned device and equipment and other IT Resources.
vi. Users must not intentionally degrade or disrupt BCIT Information Processing Facilities, including by excessive or monopolistic use of shared resources such as disk space, network bandwidth, and processing capacity. Users are responsible for communicating their resource requirements to system owners when necessary.

10. Records

When using BCIT IT Resources, employees and external service providers are responsible for submitting relevant records to the designated BCIT records custodian in accordance with Policy 6701, Records Management. This custodian ensures that records are stored in the appropriate designated repository; that their lifecycle is managed in accordance with BCIT's Directory of Records; and all practices align with the guidelines outlined in Policy 6701, Records Management.

11. Personal Use

i. BCIT's information technology assets are intended for approved BCIT purposes, including educational, academic, administrative, and research.
ii. Users are discouraged from engaging in the use of BCIT IT Resources for personal purposes and are expected to make reasonable efforts to minimize incidental personal use of BCIT IT Resources.
iii. Any personal use of BCIT IT Resources by users must not take place during an employee's working time, and must not increase the BCIT's costs, expose the BCIT to additional risk, damage BCIT's reputation, or result in personal profit.
iv. Users should also be aware that BCIT does not guarantee the security or retention of any personal content that is stored on BCIT IT Resources. BCIT assumes no responsibility for the retention or

maintenance of such personal content, and users are responsible for maintaining their own back-up copies of such data.

v. The privacy and confidentiality of a user's personal content stored on BCIT IT Resources is also not guaranteed. BCIT IT Resources are subject to routine monitoring, access and inspection as described in this Policy, and such personal content may be accessed or accessible during such activities.

vi. Privately-owned software and non-BCIT information are solely the responsibility of the User and will not be migrated when new computer systems are deployed. Any issues resulting from the use of privately-owned software installed on an BCIT asset will result in removal of the software

vii. BCIT reserves the right to manage the storage capacity and system performance of Institute-managed systems to ensure their ongoing reliability, and security. Non-business or unauthorized content may be removed if it interferes with normal operations or storage availability. This provision is not intended to affect authorized academic, instructional, research, or partnership data stored on BCIT systems. Where feasible, users will be notified or consulted before any action is taken that could impact such data.

viii. BCIT email addresses and communications should not be used for conducting personal correspondence or for signing up for personal social media accounts or non-authorized services.

12. Commercial Use

BCIT technology resources are primarily intended to support educational services, academic activity, research, and administrative functions. Use of these resources to support a user's own commercial, business, external consulting, or profit-generating activities is not permitted unless such use is part of an approved academic or research initiative (including industry-sponsored projects or cooperative work experience) and has received written authorization from the Vice President with responsibility for the user's program or department.

13. Harassment and Prohibited Conduct

i. BCIT is committed to maintaining a respectful and inclusive learning and working environment where the individual differences of all students and employees are valued, consistent with Policy 7507, Prevention of Discrimination, Harassment, and Bullying.

ii. Users are prohibited from using BCIT Information Assets or electronic communication systems to transmit, display, or store any material that is harassing, offensive, threatening, defamatory, pornographic, or obscene, except where such material is required in the context of making a formal complaint under Policy 7507.

iii. Users must not engage in any behavior using BCIT IT Resources that contravenes Policy 7507, Prevention of Discrimination, Harassment, and Bullying or any related BCIT policies.

14. Inappropriate Material

Users are prohibited from downloading, displaying, or distributing sexually explicit or violent images, video, or audio recordings using BCIT IT Resources. Users must not use BCIT IT Resources to initiate or respond to unsolicited communication containing sexual or violent content. Reference BCIT Policy 7103, Sexualized Violence.

15. Responsible Use of Social Media

Users who access and use social media platforms in connection with BCIT programs or activities are expected to demonstrate good judgment and refrain from any use that is inconsistent with this Policy or other BCIT policies. Users must comply with the following:

i. Use of social media platforms on behalf of, or in connection with, BCIT programs or activities must uphold the principles of security, confidentiality, and integrity and comply with BCIT policies.
ii. Only authorized staff may manage official BCIT social media accounts, and all activities must comply with BCIT Policy 3502, as well as relevant privacy and communications policies.
iii. Users must not make personal statements on social media that directly or indirectly imply the statement are made on behalf of or have been endorsed by BCIT.
iv. Users must protect approved BCIT social media accounts using strong passwords and authentication methods, must not disclose sensitive or confidential information, and must remain vigilant against social engineering, phishing, and other cyber threats.
v. Users are expected to use social media in compliance with FIPPA and applicable intellectual property laws, including by refraining from uploading, sharing, distributing or using content or materials that infringe upon the intellectual property rights of others.

16. Use of Official Communication Tools

BCIT-approved communication platforms—including email, voice services, and collaboration tools such as Microsoft Teams ("Communication Tools")—are designated for official administrative, academic, and research-related correspondence.

i. When using the Communication Tools, Users must follow secure communication practices in alignment with BCIT Policy 3502.
ii. All users are responsible for regularly monitoring and maintaining their official BCIT email accounts and other authorized communication channels to ensure secure and timely receipt of important information. This includes managing inbox storage, maintaining access credentials, and preventing message loss due to internal forwarding, misconfiguration, or neglect.
iii. Use of Communication Tools must comply with the requirements of this Policy, including in relation to unauthorized, commercial, personal and ethical use.

17. Responsible use of Artificial Intelligence

BCIT recognizes that artificial intelligence tools, including generative AI ("AI Tools") can support research, teaching, administration, and learning activities when used responsibly, but to mitigate risk or harmful effects they must be used in ways that uphold academic integrity, ethical decision-making, privacy, and Institute values.

When used in connection with BCIT initiatives, programs, instruction or other activities involving BCIT IT Resources, the use of AI Tools must align with BCIT's policies and security standards, and with applicable laws. In this context, all Users of AI Tools must comply with the following:

i. All proposed use of AI Tools in connection with teaching or research must be disclosed to the BCIT Information Access and Privacy Office for the completion of a Privacy and Security Threshold Assessment (PSTA).
ii. AI Tools may not be used to compile, process, assess, analyze, store or transmit BCIT Confidential Information or Personal Information unless approved in writing by BCIT. Entering or uploading student information, research data, internal documents, or any confidential content into unapproved AI Tools is strictly prohibited.
iii. Users remain responsible for all work they produce when assisted by AI Tools.
iv. All use of AI Tools must be consistent with BCIT policies and values related to equity and inclusion and must not be used to perpetrate bias or discrimination.
v. Users must review all AI-generated content for accuracy, bias, copyright compliance, and appropriateness before use or dissemination.

18. Use of BCIT-Issued Devices During International Travel

Removing BCIT Data or BCIT IT Resources for the purposes of work related or personal travel creates privacy and security risks. Users must comply with guidance issued by IT from time to time regarding the access to or use of IT Resources in connection with out-of-country travel.

Forms Associated with This Policy

None

Amendment History

			Approval Date	Status
1.	Creation:	Policy 3501 version 1	1997 Dec 01	Replaced
2.	Revision:	Policy 3501 version 2	2002 Jul 01	Replaced
3.	Revision:	Policy 3501 version 3	2003 Aug 01	Replaced
4.	Revision:	Policy 3501 version 4	2006 Aug 31	Replaced
5.	Revision:	Policy 3501 version 5	2009 May 20	Replaced
6.	Revision:	Policy 3501 version 6	2020 May 26	In Force
7.	Revision	Policy 3501 version 7	2025 [tbd]	review

Scheduled Review Date

2030 Dec 02 [***pending approval***]**. This policy must be reviewed no later than five years from approval. However, it may be updated as needed to address emerging threats and changes in technology or regulatory requirements.**

Related Documents and Legislation

Law/Regulatory/Policies	Document Name
Legislation	British Columbia *College and Institute Act*, RSBC 1996, c 52

	Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 [FIPPA] *Personal Information Protection Act*, SBC 2003, c 63 *Human Rights Code*, RSBC 1996, c 210
	Canada *Criminal Code*, RSC 1985, c C-46 *Copyright Act*, RSC 1985, c C-43
BCIT Policies	1100, Public Interest Disclosure & Protection 1200, Fraud 1300, Enterprise Risk Management 1500, Code of Conduct 3502, Information Security 5102, Student Code of Conduct (Non-Academic) 5900, Education Technology 6700, Freedom of Information and Protection of Privacy 6701, Records Management 7100, Safety and Security 7103, Sexualized Violence 7110, Emergency Management 7170, Protection of Equipment and Property 7506, Use of Materials Protected by Copyright 7507, Prevention of Discrimination, Harassment & Bullying 7511, Employment and Educational Equity

Definitions

Term	Definition
Access	The authorized ability to use, read, enter, modify, communicate with, or otherwise interact with information, systems, applications, networks, or data. Access may be physical (entry to secure facilities or server rooms) or logical (digital permissions granted through authentication and authorization).
AI	Artificial Intelligence
BCIT Data	Means Personal Information and Confidential Information.
BCIT IT Resources	Any device, system, software, application, data, or network component that is owned, leased, or managed by BCIT, or otherwise used to store, process, transmit, or secure institutional information. IT Assets include computing devices, servers, mobile equipment, cloud and network services, and digital information repositories that support BCIT's teaching, learning, research, and administrative operations.

Term	Definition
Digital Tool	Any application, platform, website, software, or online service—whether locally installed, cloud-based, or web-hosted—enabling users to create, access, process, communicate, or share digital information. Digital tools include, but are not limited to, learning management systems, collaboration platforms, productivity applications, research or data analysis tools, generative AI platforms, and open-source or commercial software used in teaching, learning, research, and administration.
Confidential Information	Means information about BCIT programs, systems, processes, plans, research, trade secrets and proprietary knowledge and materials that is not generally known, used or available.
Information Processing Facilities	Any information processing system, service, or infrastructure, or the physical locations housing them, including on-premise and cloud Services and other third-party providers of information processing Services. This includes computer labs, classroom technologies, computing and electronic communication devices, and Services such as modems, email, networks, and telephones.
FIPPA	Means the BC *Freedom of Information and Protection of Privacy Act,* including all regulations and amendments.
Instant Messaging	A form of real time communication between two or more people based on typed text.
Misuse	Means any use of BC IT Resources in violation of this Policy, FIPPA or other applicable laws.
Monitoring	The collection and review of technical system data for the purpose of ensuring operational integrity, cyber security, and legal compliance. Monitoring does not imply unrestricted access to user content.
Non-BCIT Information	Means recorded information in the custody and control of BCIT that has not been collected, used, stored or disposed of for the purpose of BCIT business.
Personal Devices	Means user-owned devices, including laptops, tablets and other digital devices and equipment.
Personal Information	Means any recorded information about an identifiable individual, including without limitation, students, staff, researchers, research subjects, volunteers, and visitors, other than business contact information.
Personal Use Records	Means records that do not relate to BCIT business, programs or activities that a user creates, stores or maintains through IT Resources.
Privacy Risk Assessment (PIA)	Means an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 of the *Freedom of Information and Protection of Privacy Act*.

Term	Definition
Privacy and Security Threshold Assessment (PSTA)	Means an assessment conducted by BCIT to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 of the *Freedom of Information and Protection of Privacy Act.*
Services	Includes but is not limited to email, file storage, portals, web page hosting and other web services, and other services.
Social Media Software	Any online application, platform, or tool that enables users to create and share content or participate in social networking. This includes, but is not limited to, platforms such as Facebook, X (formerly Twitter), Instagram, LinkedIn, and TikTok, as well as any internal social or collaborative tools.
User	A person who performs any action on an Information Asset.

ACCEPTABLE USE OF INFORMATION TECHNOLOGY – POLICY #3501

REDLINE

BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

Policy

Acceptable Use of Information Technology [DRAFT]

Policy No:	3501
Version:	~~6~~7
Category:	Information Management
Approval Body:	Board of Governors
Executive ~~Sponsor~~Sponsors:	~~Chief Information Officer~~VP Finance & Administration; VP People, Culture, & Inclusion
Department Responsible:	~~Information Technology Services~~Cyber Security Office
Directory of Records Class:	0650-15
Approval Date:	~~2020 MAY 26~~Pending

Policy Statement

~~The Institute provides information processing facilities to~~ This policy outlines the responsibilities of members of the BCIT ~~users to~~ community with respect to the responsible and acceptable use and security of BCIT IT Resources, which include technology, data, digital assets, systems, equipment and devices. It sets out requirements for the responsible, ethical, and legally compliant use of technology resources in support ~~the~~ of BCIT operations, teaching, research, and administrative activities.

Through this Policy, BCIT seeks to foster a secure, innovative, and collaborative digital environment supporting BCIT's teaching, learning, research, and administrative goals ~~of the Institute. These resources are valuable community assets~~. This Policy incorporates and adopts a risk-based and collaborative approach, encouraging both responsible technology use and the promotion of innovation to ~~be used and managed responsibly~~advance BCIT's academic mission. BCIT affirms its commitment to ~~ensure their integrity, security, and availability for educational and business activities.~~ the principles of academic freedom.

~~This policy applies to all Institute information and computing, communications, and networking resources connected to Institute facilities and the users of these resources.~~

Purpose of Policy

~~BCIT's information, network, and other information technology (IT) services are shared resources that are critical to teaching, learning, research, Institute operations, and service delivery.~~

The purpose of this ~~policy~~Policy is to~~:~~

- ~~Establish responsibilities regarding acceptable use of information technology for all BCIT users~~
- ~~Ensure the safe and respectful use of BCIT's information technology for all BCIT users~~

Formatted Table

Style Definition: Normal: Indent: Left: 0 cm

Style Definition: Heading 1: Font: 12 pt, English (Canada), Space Before: 0.1 pt

Style Definition: Heading 2: Font: (Default) Calibri, 11 pt, Right: 0.28 cm, Space After: 8 pt, Don't add space between paragraphs of the same style, Line spacing: Multiple 1.08 li, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1.9 cm + Indent at: 2.54 cm

Style Definition: Heading 3: Font: (Default) Calibri, 11 pt, Not Bold, Not Italic, English (Canada), Justified, Space Before: 0.1 pt, After: 12 pt, Line spacing: Multiple 1.08 li, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.63 cm + Indent at: 1.27 cm

Style Definition: TOC 1: Indent: Left: 0 cm, Tab stops: Not at 11.43 cm

Style Definition: Bullet/HeadingO1: Tab stops: Not at 13.71 cm

Style Definition: Heading 1/O: Indent: Left: 0 cm, Tab stops: Not at 3.26 cm

Style Definition: Normal (Web)

Formatted: Font: 14 pt

Formatted: Font color: Text 1

Formatted: Heading 3

Formatted: English (United States)

Formatted: English (United States)

Formatted: Space Before: 0 pt

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

Table of Contents

Who This Policy Applies To

This policy applies to everyone who accesses BCIT's information technology assets. This includes those who use their own personal equipment to connect to Institute Information Assets.

Related Documents and Legislation

Legislation

British Columbia

College and Institute Act, RSBC 1996, c 52
Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165
Personal Information Protection Act, SBC 2003, c 63
Human Rights Code, RSBC 1996, c 210

Canada

Criminal Code, RSC 1985, c C-46
Copyright Act, RSC 1985, c C-43

BCIT Policies

1504, Standards of Conduct and Conflict of Interest
3502, Information Security
5102, Student Code of Conduct (Non Academic)
6700, Freedom of Information and Protection of Privacy
6701, Records Management
7110, Emergency Management
7170, Protection of Equipment and Property
7506, Use of Materials Protected by Copyright
7507, Harassment and Discrimination
7511, Employment and Educational Equity

BCIT Procedures

3502 PR1, Information Security
7100 PR1, Response to Abusive or Threatening Behaviour

Formatted: Normal, Space Before: 0 pt

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

~~Definitions~~

~~**BCIT Internal Use:** information that is available to authorized Users and is not routinely disclosed. By default, data is BCIT Internal Use until it is assessed and otherwise classified.~~

~~**Blog:** short for "web log", is comparable to an online journal that allows Users to post thoughts, ideas, or news items.~~

~~**Confidential Information:** information that contains sensitive Institute information and is available to authorized Users. A formal FOIPOP request is required for non-routine disclosure.~~

~~**Defamation:** a communicated statement found to be false and that causes harm to someone's reputation.~~

~~**Directory of Records:** see Policy 6701, Records Management.~~

~~**E-communications:** the use of digital electronic technologies to communicate, including but not limited to, email systems, chat rooms, news groups, Blogs, Social Software, instant messaging and voice communication systems.~~

~~**Information Asset:** an asset that is comprised of digitized information or of equipment or systems, both fixed and/or mobile for the processing of information.~~

~~**Information Processing Facilities:** any information processing system, service, or infrastructure, or the physical locations housing them, including on-premise and cloud Services and other 3rd party providers of information processing Services. This includes computer labs, classroom technologies, computing and electronic communication devices, and Services such as modems, email, networks, and telephones.~~

~~**Instant Messaging:** a form of real time communication between two or more people based on typed text.~~

~~**Non-Institute Information:** information that is created and maintained by an individual for the purposes of that individual. Non-Institute information, by definition, is not classified as Personal or Confidential by the Institute, although non-Institute information may be considered personal or confidential by the owner.~~

~~**Personal Information:** information that contains sensitive personal information and is available to authorized Users only. A formal FOIPOP request is required for non-routine disclosure.~~

~~**Services:** including but not limited to email, file storage, portals, web page hosting and other web services, and other services.~~

~~**Social Software:** software whose primary purpose is to facilitate communication between individuals and groups who share a common interest. Social Software includes, but is not limited to:~~

- ~~social networking such as Instagram, Twitter and LinkedIn;~~
- ~~filesharing such as Youtube, Flickr, Dropbox, Google Docs, and Box;~~
- ~~instant messaging such as Messenger and Google Hangouts; and~~
- ~~other publishing Services such as Blogs and Wikis, and synchronous and asynchronous chat and instant messaging tools such as Skype and on-line discussion forums.~~

~~**User:** a person who performs any action on an Information Asset.~~

Formatted: Normal, Space Before: 0 pt

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

~~**Wiki:** a web-based application that allows collaborative editing of its content and structure by its Users. The ease of interaction and operation makes a wiki an effective tool for mass collaborative authoring.~~

~~Consequences of Policy Violation~~

~~The Institute reserves the right to terminate or restrict the access privileges of a User whose activities negatively affect or pose a threat to a facility, another account holder, normal operations, or the reputation of the Institute.~~

~~Following due process, the Institute may take one or more of the following actions against any User whose activities are in violation of this policy or applicable law:~~

- ~~verbal or written warnings;~~
- ~~restrictions or removal of access to Institute computing facilities and Services;~~
- ~~legal action that could result in criminal or civil proceedings;~~
- ~~for students, disciplinary action under Policy 5102, Student Code of Conduct (Non Academic); and~~
- ~~for employees, disciplinary action up to and including termination.~~

~~Equipment that violates BCIT policy or negatively affects or poses a threat to a facility, normal operations, or the reputation of the Institute may be immediately disconnected, quarantined, or otherwise contained. Institute-owned equipment may also be seized.~~

~~Duties and Responsibilities~~

~~1. Responsibilities by Role~~

~~***Board of Governors and BCIT Executive***~~

~~The BCIT Board of Governors and the BCIT Executive actively support and promote the acceptable use of information technology.~~

~~***Cyber Security Officer***~~

~~The Cyber Security Officer provides leadership and oversight over all aspects of cyber security, including cyber threat and risk management, developing and delivering an institutional cyber awareness program, security policies, procedures and standards formation and application. The Cyber Security Officer publishes and maintains the Information Security Standard and reviews it periodically in light of changing~~ establish clear expectations and ~~risks.~~

~~***BCIT Management***~~

~~Members of BCIT Management are~~ requirements for the responsible ~~for ensuring that employees~~ and ~~others under their supervision are aware of their~~ acceptable use of ~~information technology responsibilities~~BCIT IT Resources by all users.

Formatted: Heading 3

~~***Instructors and Teaching Faculty***~~

~~Instructors and Teaching Faculty are responsible for ensuring that students under their supervision are aware of their acceptable use of information technology responsibilities.~~

~~***IT Administrators***~~

~~IT Administrators~~Who This Policy Applies To

Formatted: Normal, Space Before: 0 pt

This Policy applies to all individuals who use BCIT IT Resources, including staff, faculty, students, contractors, third-party contractors, researchers, and visitors. It also applies to users who use Personal Devices in connection with BCIT IT Resources.

Consequences of Policy Violation

Compliance with this Policy is mandatory for all users of BCIT's IT Resources. Users who breach this Policy or engage in Misuse will be subject to discipline, up to and inclusive of dismissal or expulsion.

BCIT reserves the right to restrict, suspend, or withdraw access to BCIT systems and services, including computing privileges and network connectivity.

Investigations of suspected Misuse and any resulting actions will follow established Institute procedures and principles of fairness and due process.

In cases where Misuse or other ~~privileged Users must protect the~~ user equipment or activity poses an immediate security ~~of~~ or operational risk, BCIT may take temporary measures to protect Institute systems, such as disconnecting or quarantining affected devices, until the ~~information and must not abuse their elevated privileges.~~issue is investigated and resolved.

~~***System Owners***~~

~~System Owners must ensure that all Users have been made aware of this policy and Policy 3502, Information Security, prior to granting access.~~

~~***Safety, Security and Emergency Management***~~

~~The Safety and Security and Emergency Management department is responsible for monitoring the Institute's physical environment to ensure unacceptable behaviour is minimized.~~

~~***Risk Management***~~

~~The Enterprise Risk Management group is responsible for monitoring liability risk from Defamation and harassment.~~

~~***Users***~~

~~All Users are responsible for:~~

- ~~familiarizing themselves with their responsibilities;~~
- ~~complying with Policy 3502, Information Security, and other applicable Institute policies;~~
- ~~complying with this Policy 3501, Acceptable Use of Information Technology; and~~
- ~~promptly reporting any act that may constitute a real or suspected breach of acceptable use of information technology.~~

Person Device connecting to BCIT networks may also be subject to reasonable security restrictions to protect Institute systems and data integrity.

Duties and Responsibilities

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

Formatted: Heading 3

Formatted: Normal, Space Before: 0 pt

Role	Responsibilities
Board of Governors and BCIT Executive	The BCIT Board of Governors and the BCIT Executive actively support and promote the acceptable use of information technology.
Chief Information Security Officer (CISO)	The CISO provides leadership and oversight for the security of BCIT's IT systems, data, and digital assets. Their responsibilities include developing and enforcing security policies and standards, ensuring compliance with applicable regulations, and maintaining a secure and resilient infrastructure capable of detecting, preventing, and responding to cyber threats. The CISO also serves as the final authority for approving security exceptions.
BCIT Management	Members of BCIT Management are responsible for ensuring that staff and others under their supervision are aware of their responsibilities for the acceptable use of information technology.
Instructors and Teaching Faculty	Instructors and Teaching Faculty are responsible for ensuring that students under their supervision are aware of their responsibilities for the acceptable use of information technology.
IT Administrators	IT Administrators and other privileged Users must protect the security of BCIT It Resources and must not abuse their elevated privileges.
Safety, Security and Emergency Management	The Safety and Security and Emergency Management department is responsible for monitoring BCIT's physical environment to ensure Misuse and other unacceptable behaviour is minimized.
Risk Management	The Enterprise Risk Management group is responsible for monitoring liability risk associated with the use and Misuse of BCIT IT Resources.
Users	All Users are responsible for familiarizing themselves with their responsibilities under this Policy. Users should promptly report known or suspected instances of Misuse.

~~2.~~1. General Accountability

~~By using Institute Information Processing Facilities or any Information Assets, Users accept the terms of this policy and Policy 3502, Information Security.~~

All use of BCIT IT Resources is subject to compliance with this Policy. It is the responsibility of all users to ensure they are familiar with and comply with this Policy.

~~3.~~2. Access

~~See Policy 3502, Information Security.~~

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

Formatted: Heading 2, Indent: Left: 0.76 cm, Don't keep with next

Formatted: Heading 2, Indent: Left: 0.75 cm, Don't keep with next

Formatted: Normal, Space Before: 0 pt

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

~~4. Copyright~~

~~All electronic data including software, music, video, and audio media that are transmitted or stored on~~BCIT's IT Resources may be accessed and used only by members of the BCIT community who are granted access privileges by BCIT. All access and use are subject to compliance with this Policy, other applicable BCIT Policies, including Policy 3502 Cyber Security, and with the applicable laws of British Columbia and Canada, including the *Criminal Code*, the *Copyright Act*, the *Human Rights Code* and FIPPA.

3. Copyright and Intellectual Property

When using BCIT IT Resources, users must comply with all applicable laws and Institute ~~Information Processing Facilities are subject to Policy 7506~~policies related to intellectual property and copyright, including BCIT Policy 7505, Use of ~~Materials~~Material Protected by Copyright, ~~and the *Copyright Act* (Canada).~~

Formatted: Heading 3, Indent: Left: 0.75 cm

~~Users may be required to obtain permission~~including by refraining from ~~the copyright owners for the digitizing, storing, sharing, and transmission of~~ any acts that infringe upon copyright ~~protected materials. Users must not use BCIT's Information Processing Facilities to receive, store, share, or send any unauthorized materials.~~ in relation to computer programs, data collection, work product, and any literary, dramatic, artistic and musical work.

Formatted: Font: 12 pt

~~5.~~4. Usage and Monitoring

Formatted: Heading 2, Indent: Left: 0.75 cm, Don't keep with next

~~The Institute regularly monitors its assets, and all non-Institute information transferred or stored on Institute assets may be reviewed as a result of this routine monitoring activity; Users should have no expectation of privacy regarding any Institute or non-Institute information stored on or transmitted using Institute assets.~~

~~Students using computer lab facilities during scheduled class time~~BCIT monitors the use of its IT Resources for operational, security, and compliance purposes. Monitoring supports the protection of BCIT Data, detection and response to cyber security threats, and compliance with legal, policy and regulatory obligations. Users should understand that this monitoring and maintenance may involve access to Personal Use Records or Personal Information of users.

i. BCIT makes reasonable efforts to ensure monitoring activities are limited to what is necessary and proportionate to achieve the above purposes and are conducted in compliance with applicable legislation, including FIPPA.

ii. Users should be aware that information created, transmitted, or stored using BCIT IT Resources may be subject to ~~monitoring at the instructor's discretion. Use of computer lab facilities at~~access or review under circumstances such as:

   a. a suspected or confirmed security or policy incident;
   b. an investigation under Institute, legislative, policy or legal authority; or,
   c. routine system performance or security assurance activities.

Formatted: Normal, Space Before: 0 pt

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

iii. BCIT will not intentionally access, use or disclose Personal Information or personal records stored on BCIT IT Resources without the user's knowledge and consent unless:
   a. authorized or required by law,
   b. where securing the user's consent would compromise the health and safety of any ~~time is~~ individual or group; or,
   c. where the information is needed for an investigation or proceeding related to a breach of law, policy or employment duties and seeking consent would compromise the availability of required information or the investigation or proceeding.

iv. BCIT also reserves the right to access information or communications stored on BCIT IT Resources where needed to transition employment responsibilities after an employee departs from their employment or is on an extended leave.

v. Access requests involving intentional access to a user's Personal Information or Personal Use Records stored on BCIT IT Resources must be pre-authorized by the Chief Information Security Officer or their designate. Where applicable, such access will also be subject to ~~the~~ oversight and approval from the Information Access and Privacy Office and/or the Human Resources department to ensure compliance with privacy, legal, and organizational requirements.

vi. BCIT recognizes the importance of privacy, academic freedom, and the confidentiality of research data. Routine monitoring of IT Resources does not involve intentional access to research data, academic work, or personal communications except as described in this Policy.

vii. Personal Devices are not subject to routine monitoring ~~activities.~~. However, network activity from Personal Devices connected to BCIT systems may be logged to detect anomalies, threats, or policy violations.

Formatted: Heading 3, Indent: Left: 1 cm, Hanging: 0.26 cm, Don't add space between paragraphs of the same style, Numbered + Level: 1 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Right + Aligned at: 0.63 cm + Indent at: 1.27 cm

viii. All monitoring and logging activities are recorded, audited, and subject to appropriate oversight and accountability.

~~6.~~5. Connecting Equipment to the BCIT Network

Formatted: Heading 2, Indent: Left: 0.76 cm, Don't keep with next

~~When connecting~~ Users are subject to the following requirements regarding devices and equipment ~~to the~~ :

i. BCIT ~~-~~owned and managed equipment, including desktops, laptops, mobile devices, servers, and network~~, Users are responsible for adhering to this policy and~~ enabled systems, must comply with Policy 3502, Cyber Security and cyber security standards and requirements. These devices are centrally managed and monitored by IT Services to ensure appropriate patching, antivirus protection, and security configurations.

ii. The use of Personal Devices is permissible to enhance learning, teaching, and productivity, provided that such use does not create risks to the security, privacy, and integrity of BCIT IT Resources. BCIT reserves the right to restrict or impose conditions or security controls on the use of Personal Devices where necessary to protect BCIT IT Resources.

Formatted: Normal, Space Before: 0 pt

iii. Recognizing that academic programs and research projects often involve testing or deploying specialized technologies, faculty and research teams may connect experimental or instructional devices (including IoT or prototype systems) to approved lab or research networks. Such connections must be coordinated with the Cyber Security Office to ensure that security controls and network configurations protect both the research environment and the broader campus network.

iv. Internet of Things (IoT) devices (e.g., smart TVs, sensors) intended for use in buildings and in research or academic labs must be registered and approved by IT Services prior to connection. IoT devices used solely for instructional or research purposes may be connected to isolated or sandbox environments with appropriate safeguards and faculty oversight.

v. To maintain a secure and reliable technology environment, BCIT may implement reasonable measures to safeguard network performance, data integrity, and BCIT systems. These measures may include monitoring, restricting, or temporarily disconnecting devices—whether BCIT-owned, personal, or research-related—if they are determined to pose a security or operational risk to BCIT.

6. Use of BCIT Information ~~Security~~ on Non-BCIT Equipment

BCIT recognizes that users may need to access BCIT enterprise systems or communication tools from Personal Devices such as smartphones, tablets, and laptops. To protect BCIT Data while maintaining flexibility, Personal Device use is permitted under the following conditions:

i. Devices must be protected by secure login and comply with any applicable BCIT access control policies.

ii. Devices must use current operating system updates, and full-disk encryption.

iii. Users must not store or transmit sensitive Personal Information or Confidential Information on Personal Devices unless explicitly authorized by their supervisor, and in such circumstances, data must be encrypted.

iv. Personal Devices on which BCIT Confidential Information or Personal Information is stored may not be removed from Canada unless such data has been securely and permanently wiped from the device or it is otherwise permitted under this Policy.

v. BCIT files must not be synchronized to unmanaged or personal cloud storage applications.

vi. Users must not disable, bypass, or circumvent BCIT security controls, including MFA prompts or device compliance ~~may result in immediate disconnection from the network~~checks.

~~Connection of non-Institute computer equipment to Institute Information Processing Facilities is subject to Policy 3502, Information Security. All equipment connected to the network is governed by Institute policies and may be monitored for compliance.~~

~~7. Use of Institute Information on Non-Institute Equipment~~

~~If an employee, student or external party stores, processes or accesses Personal, Confidential or BCIT Internal Use information on non-Institute equipment, the User and the~~

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

Formatted: Heading 3, Indent: Left: 0.99 cm, Hanging: 0.25 cm, Don't add space between paragraphs of the same style, Numbered + Level: 1 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Right + Aligned at: 2.67 cm + Indent at: 3.3 cm

Formatted: Normal, Space Before: 0 pt

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

~~equipment must comply with this policy, Policy 3502, Information Security, as well as the Information Security Standard 3502.~~

~~8. Off-Campus Use of Institute Equipment~~

~~Authorized Users of off-campus Institute-owned equipment are bound by this policy and Policy 3502, Information Security.~~

vii. BCIT Data must be securely deleted from Personal Devices once no longer needed.

viii. Any lost, stolen, or compromised Personal Devices used for BCIT purposes must be reported immediately to IT Services or the Cyber Security Office.

ix. BCIT reserves the right to restrict or revoke access if a personal device poses a security or compliance risk to BCIT systems or data.

x. Users of Personal Devices maintaining or storing BCIT records or information may be required, upon request, to provide copies of all such records to BCIT and/or to securely delete them from Personal Devices.

~~9.~~7. Personal Information Collection and Use

Formatted: Heading 2, Indent: Left: 0.75 cm, Don't keep with next

The collection, use, storage, and transmission of ~~personal information are~~Personal Information is governed by Policy 6700, Freedom of Information and Protection of Privacy, and Policy 3502, ~~Information~~Cyber Security.

Formatted: Font: +Body (Calibri)

Formatted: Font: +Body (Calibri)

Formatted: Font: +Body (Calibri)

Formatted: Font: +Body (Calibri)

In accordance with FIPPA, Users are required to ~~contact~~complete a Privacy and Security Threshold Assessment (PSTA) before implementing new initiatives, systems, programs or projects that involve the use or processing of Personal Information ~~Access and Privacy Office prior to collection of personal information.~~.

Formatted: Heading 3, Indent: Left: 0.75 cm

~~10.~~8. Responsible Use of Software and Digital Tools

Formatted: Heading 2, Indent: Left: 0.75 cm, Don't keep with next

~~All software installed on Institute-owned Information Assets must be properly licensed. Users~~ BCIT supports innovation in the use of digital tools and resources. Users may explore and use digital tools to enhance academic, research, and administrative activities. Software and applications that process, store, or transmit BCIT Data must comply with BCIT's security standards and licensing requirements, and be used in accordance with Policy 3502, Cyber Security.

i. BCIT supports the responsible use of open-source, open-educational, and cloud-based tools, provided they comply with BCIT's security standards, licensing requirements, and with Policy 3502, Cyber Security and Policy 5900, Educational Technology.

ii. Users must consult IT Services or the Cyber Security Office before adopting new digital tools for teaching or research that may involve the use of BCIT enterprise systems, cloud, or data, including where they involve the collection, use or disclosure of Personal Information BCIT employees or students.

Formatted: Normal, Space Before: 0 pt

iii. Downloading or installing unverified or unlicensed software to IT Resources is prohibited due to potential risks to security, compliance, privacy, and data integrity.

9. Responsible Use of Hardware Assets

Users are responsible for their own use of devices and equipment in compliance with this Policy, other applicable BCIT policies, and applicable laws. In addition, where applicable users must comply with the following requirements.

i. All users are required to use BCIT-owned IT assets securely, ethically, and in alignment with authorized academic, research, administrative, or operational activities, in compliance with BCIT policies, legal requirements, and cyber security best practices.
ii. BCIT-owned equipment (e.g., laptops, mobile devices, external drives) may be used off-campus by authorized users, provided appropriate security measures are in place to protect BCIT Data and assets. Users must take reasonable steps to prevent unauthorized access, loss, theft or Misuse of devices, including secure handling, storage, and prompt reporting of any incidents of loss, theft or device compromise.
iii. BCIT equipment remains the property of BCIT and must be returned upon request or at the end of employment, contract, or academic term.
iv. Personal Devices must not be used in ways that jeopardize the security or integrity of BCIT Data or BCIT IT Resources.
v. Users are prohibited from ~~using Institute~~unauthorized modification, tampering, or Misuse of BCIT owned device and equipment and other IT Resources.
vi. Users must not intentionally degrade or disrupt BCIT Information Processing Facilities ~~or Information Assets to download, store, use, or distribute unlicensed software~~, including by excessive or monopolistic use of shared resources such as disk space, network bandwidth, and processing capacity. Users are responsible for communicating their resource requirements to system owners when necessary.

~~11.~~10. Records

When using ~~Institute Information Assets~~BCIT IT Resources, employees and external ~~parties who provide Services~~service providers are responsible for ~~identifying BCIT official records and~~ submitting ~~those~~relevant records to the designated ~~repository according to the Directory of Records as detailed~~BCIT records custodian in accordance with Policy 6701, Records Management. This custodian ensures that records are stored in the appropriate designated repository; that their lifecycle is managed in accordance with BCIT's Directory of Records; and all practices align with the guidelines outlined in Policy 6701, Records Management.

~~12.~~11. Personal Use

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

Formatted: Heading 3, Indent: Left: 0.99 cm, Hanging: 0.25 cm, Don't add space between paragraphs of the same style, Numbered + Level: 2 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Right + Aligned at: 0.63 cm + Indent at: 1.27 cm

Formatted: Heading 2, Indent: Left: 0.76 cm, Don't keep with next

Formatted: Heading 3, Indent: Left: 0.75 cm

Formatted: Heading 2, Indent: Left: 0.76 cm, Don't keep with next

Formatted: Normal, Space Before: 0 pt

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

i. BCIT's information technology assets are intended for approved InstituteBCIT purposes (, including educational, academic, administrative, and research). All .
ii. Users must are discouraged from engaging in the use of BCIT IT Resources for personal purposes and are expected to make reasonable efforts to minimize incidental personal use of Institute Information Assets. Such personal useBCIT IT Resources.
iii. Any personal use of BCIT IT Resources by users must not take place during an employee's working time, and must not increase the Institute'sBCIT's costs, expose the InstituteBCIT to additional risk, damage the Institute'sBCIT's reputation, or result in personal profit.

Formatted: Heading 3, Indent: Left: 0.99 cm, Hanging: 0.25 cm, Don't add space between paragraphs of the same style, Numbered + Level: 1 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Right + Aligned at: 0.63 cm + Indent at: 1.27 cm

iv. Users should also be aware that BCIT does not guarantee the security or retention of any personal content that is stored on BCIT IT Resources. BCIT assumes no responsibility for personal E-communications using Institute assets. Users must not misrepresentthe retention or maintenance of such personal E-communicationscontent, and users are responsible for maintaining their own back-up copies of such data.
v. The privacy and confidentiality of a user's personal content stored on BCIT IT Resources is also not guaranteed. BCIT IT Resources are subject to routine monitoring, access and inspection as official Institute E-communicationsdescribed in this Policy, and such personal content may be accessed or accessible during such activities.

Formatted: Heading 3, Indent: Left: 0.99 cm, Hanging: 0.25 cm, Don't add space between paragraphs of the same style, Numbered + Level: 1 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Right + Aligned at: 0.63 cm + Indent at: 1.27 cm

vi. Privately-owned software and non-InstituteBCIT information isare solely the responsibility of the User and will not be migrated when new computer systems are deployed. Any issues resulting from the use of privately-owned software installed on an InstituteBCIT asset will result in removal of the software.

Formatted: Heading 3, Indent: Left: 0.99 cm, Hanging: 0.25 cm, Don't add space between paragraphs of the same style, Numbered + Level: 1 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Right + Aligned at: 0.63 cm + Indent at: 1.27 cm

The Institute reserves the right to remove non-Institute information from storage without warning or terminate or otherwise limit the transmission of non-Institute information without warning if the storage or transmission interferes with normal operations.

vii. BCIT reserves the right to manage the storage capacity and system performance of Institute-managed systems to ensure their ongoing reliability, and security. Non-business or unauthorized content may be removed if it interferes with normal operations or storage availability. This provision is not intended to affect authorized academic, instructional, research, or partnership data stored on BCIT systems. Where feasible, users will be notified or consulted before any action is taken that could impact such data.
viii. BCIT email addresses and communications should not be used for conducting personal correspondence or for signing up for personal social media accounts or non-authorized services.

13.12. Commercial Use

Formatted: Heading 2, Indent: Left: 0.76 cm, Don't keep with next

All use of Institute Information Assets for any business or commercial purposes must be authorized by the Institute.

Formatted: Normal, Space Before: 0 pt

BCIT technology resources are primarily intended to support educational services, academic activity, research, and administrative functions. Use of these resources to support a user's own commercial, business, external consulting, or profit-generating activities is not permitted unless such use is part of an approved academic or research initiative (including industry-sponsored projects or cooperative work experience) and has received written authorization from the Vice President with responsibility for the user's program or department.

~~14.~~13. Harassment and Prohibited Conduct

i. BCIT is committed to ~~providing a~~ maintaining a respectful and inclusive learning and working environment where the individual differences of all students and employees are valued ~~and respected as per~~, consistent with Policy 7507, ~~Harassment and~~ Prevention of Discrimination~~.~~, Harassment, and Bullying.

ii. Users ~~must not send~~are prohibited from using BCIT Information Assets or electronic communication systems to transmit, display, or store any material that is harassing, offensive, threatening, defamatory, pornographic, or obscene ~~material by E-communications using Institute Information Assets~~, except where such material is required in the context of making a formal complaint~~.~~ under Policy 7507.

iii. Users must not engage in any behavior using BCIT IT Resources that contravenes Policy 7507, Prevention of Discrimination, Harassment, and Bullying or any related BCIT policies.

~~15.~~14. Inappropriate Material

~~All~~ Users are prohibited from downloading, displaying, or distributing sexually explicit or violent images, video, or audio recordings~~.~~ using BCIT IT Resources. Users ~~shall~~must not use BCIT IT Resources to initiate or respond to unsolicited communication containing sexual or violent content. Reference BCIT Policy 7103, Sexualized Violence.

~~This provision does not apply to the residence zone.~~

~~16. Responsible Use of Assets~~

~~Users must not deliberately degrade Institute Information Processing Facilities or deny service to others through any actions including excessive consumption or locking of resources including disk space, network bandwidth, and printing and processing capacity. Users have an obligation to inform system owners of their capacity requirements.~~

~~17.~~15. Responsible Use of Social Media

~~Users should refrain from including sensitive business information in the business or personal profile or posts on social media sites. Social networking sites like Facebook, Twitter and LinkedIn can be powerful tools for any business to reach potential audience but are also~~

Formatted Table
Formatted: Font: 2 pt
Formatted: Header, Tab stops: 2.11 cm, Left
Formatted: Normal
Formatted: Heading 2, Indent: Left: 0.76 cm, Don't keep with next
Formatted: Heading 3, Indent: Left: 0.99 cm, Hanging: 0.25 cm, Don't add space between paragraphs of the same style, Numbered + Level: 1 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Right + Aligned at: 0.63 cm + Indent at: 1.27 cm
Formatted: Heading 2, Indent: Left: 0.76 cm
Formatted: Font: +Body (Calibri), Bold
Formatted: Heading 2, Indent: Left: 0.76 cm, Don't keep with next
Formatted: Normal, Space Before: 0 pt

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

~~becoming an increasingly popular way for cyber criminals to try to get your personal or business information to hack into your personal or business enterprise systems.~~

~~**18. Use of Email for Official Communications**~~

~~Email is an official communication mechanism of the Institute. All Users must adhere to safe email practices as per Policy 3502, Information Security.~~

~~Users are responsible for ensuring that they can review official Institute emails in a timely manner. This includes account monitoring, management of storage space, and ensuring mail is flowing to any forwarded internal address.~~

~~**19. Use of Voicemail**~~

~~The BCIT voicemail system is for Institute business only. Greetings and messages must not convey or promote an employee's personal interest or private business.~~

~~Employees are responsible for managing their voicemail messages effectively. See Procedure 3502-PR1, Information Security, for details.~~

~~Procedures Associated With This Policy~~

~~Procedure 3502-PR1, Information Security~~

Users who access and use social media platforms in connection with BCIT programs or activities are expected to demonstrate good judgment and refrain from any use that is inconsistent with this Policy or other BCIT policies. Users must comply with the following:

i. Use of social media platforms on behalf of, or in connection with, BCIT programs or activities must uphold the principles of security, confidentiality, and integrity and comply with BCIT policies.
ii. Only authorized staff may manage official BCIT social media accounts, and all activities must comply with BCIT Policy 3502, as well as relevant privacy and communications policies.
iii. Users must not make personal statements on social media that directly or indirectly imply the statement are made on behalf of or have been endorsed by BCIT.
iv. Users must protect approved BCIT social media accounts using strong passwords and authentication methods, must not disclose sensitive or confidential information, and must remain vigilant against social engineering, phishing, and other cyber threats.
v. Users are expected to use social media in compliance with FIPPA and applicable intellectual property laws, including by refraining from uploading, sharing, distributing or using content or materials that infringe upon the intellectual property rights of others.

16. Use of Official Communication Tools

BCIT-approved communication platforms—including email, voice services, and collaboration tools such as Microsoft Teams ("Communication Tools")—are designated for official administrative, academic, and research-related correspondence.

i. When using the Communication Tools, Users must follow secure communication practices in alignment with BCIT Policy 3502.

Formatted: Normal, Space Before: 0 pt

ii. All users are responsible for regularly monitoring and maintaining their official BCIT email accounts and other authorized communication channels to ensure secure and timely receipt of important information. This includes managing inbox storage, maintaining access credentials, and preventing message loss due to internal forwarding, misconfiguration, or neglect.

iii. Use of Communication Tools must comply with the requirements of this Policy, including in relation to unauthorized, commercial, personal and ethical use.

17. Responsible use of Artificial Intelligence

BCIT recognizes that artificial intelligence tools, including generative AI ("AI Tools") can support research, teaching, administration, and learning activities when used responsibly, but to mitigate risk or harmful effects they must be used in ways that uphold academic integrity, ethical decision-making, privacy, and Institute values.

When used in connection with BCIT initiatives, programs, instruction or other activities involving BCIT IT Resources, the use of AI Tools must align with BCIT's policies and security standards, and with applicable laws. In this context, all Users of AI Tools must comply with the following:

i. All proposed use of AI Tools in connection with teaching or research must be disclosed to the BCIT Information Access and Privacy Office for the completion of a Privacy and Security Threshold Assessment (PSTA).

ii. AI Tools may not be used to compile, process, assess, analyze, store or transmit BCIT Confidential Information or Personal Information unless approved in writing by BCIT. Entering or uploading student information, research data, internal documents, or any confidential content into unapproved AI Tools is strictly prohibited.

iii. Users remain responsible for all work they produce when assisted by AI Tools.

iv. All use of AI Tools must be consistent with BCIT policies and values related to equity and inclusion and must not be used to perpetrate bias or discrimination.

v. Users must review all AI-generated content for accuracy, bias, copyright compliance, and appropriateness before use or dissemination.

18. Use of BCIT-Issued Devices During International Travel

Removing BCIT Data or BCIT IT Resources for the purposes of work related or personal travel creates privacy and security risks. Users must comply with guidance issued by IT from time to time regarding the access to or use of IT Resources in connection with out-of-country travel.

Forms Associated ~~With~~with This Policy

None

Amendment History

		Approval Date	Status
1. Creation:	Policy 3501 version 1	1997 Dec 01	Replaced

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

Formatted: Font: +Body (Calibri), 11 pt, Not Bold

Formatted: Heading 1, Indent: First line: 1.27 cm

Formatted: Font: +Body (Calibri), 11 pt

Formatted: Indent: Left: 2.54 cm, Right: 0.27 cm, Space Before: 0.1 pt, After: 0.1 pt

Formatted: Normal, Space Before: 0 pt

2.	Revision:	Policy 3501 version 2	2002 Jul 01	Replaced
3.	Revision:	Policy 3501 version 3	2003 Aug 01	Replaced
4.	Revision:	Policy 3501 version 4	2006 Aug 31	Replaced
5.	Revision:	Policy 3501 version 5	2009 May 20	Replaced
6.	Revision:	Policy 3501 version 6	2020 May 26	In Force
7.	Revision	Policy 3501 version 7	2025 [tbd]	review

Scheduled Review Date

~~2025 May 26~~

2030 Dec 02 [***pending approval***]**. This policy must be reviewed no later than five years from approval. However, it may be updated as needed to address emerging threats and changes in technology or regulatory requirements.**

Related Documents and Legislation

Law/Regulatory/Policies	Document Name
Legislation	British Columbia *College and Institute Act*, RSBC 1996, c 52 *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 [FIPPA] *Personal Information Protection Act*, SBC 2003, c 63 *Human Rights Code*, RSBC 1996, c 210
	Canada *Criminal Code*, RSC 1985, c C-46 *Copyright Act*, RSC 1985, c C-43
BCIT Policies	1100, Public Interest Disclosure & Protection 1200, Fraud 1300, Enterprise Risk Management 1500, Code of Conduct 3502, Information Security 5102, Student Code of Conduct (Non-Academic) 5900, Education Technology 6700, Freedom of Information and Protection of Privacy 6701, Records Management 7100, Safety and Security 7103, Sexualized Violence 7110, Emergency Management 7170, Protection of Equipment and Property 7506, Use of Materials Protected by Copyright 7507, Prevention of Discrimination, Harassment & Bullying

Formatted Table
Formatted: Font: 2 pt
Formatted: Header, Tab stops: 2.11 cm, Left
Formatted: Normal
Formatted: Font: +Body (Calibri), 11 pt
Formatted: Font: +Body (Calibri), 11 pt
Formatted: Font: +Body (Calibri), 11 pt
Formatted: Font: +Body (Calibri), 11 pt
Formatted: Font: +Body (Calibri)
Formatted: Normal, Space Before: 0 pt

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

	7511, Employment and Educational Equity

Definitions

Term	Definition
Access	The authorized ability to use, read, enter, modify, communicate with, or otherwise interact with information, systems, applications, networks, or data. Access may be physical (entry to secure facilities or server rooms) or logical (digital permissions granted through authentication and authorization).
AI	Artificial Intelligence
BCIT Data	Means Personal Information and Confidential Information.
BCIT IT Resources	Any device, system, software, application, data, or network component that is owned, leased, or managed by BCIT, or otherwise used to store, process, transmit, or secure institutional information. IT Assets include computing devices, servers, mobile equipment, cloud and network services, and digital information repositories that support BCIT's teaching, learning, research, and administrative operations.
Digital Tool	Any application, platform, website, software, or online service—whether locally installed, cloud-based, or web-hosted—enabling users to create, access, process, communicate, or share digital information. Digital tools include, but are not limited to, learning management systems, collaboration platforms, productivity applications, research or data analysis tools, generative AI platforms, and open-source or commercial software used in teaching, learning, research, and administration.
Confidential Information	Means information about BCIT programs, systems, processes, plans, research, trade secrets and proprietary knowledge and materials that is not generally known, used or available.
Information Processing Facilities	Any information processing system, service, or infrastructure, or the physical locations housing them, including on-premise and cloud Services and other third-party providers of information processing Services. This includes computer labs, classroom technologies, computing and electronic communication devices, and Services such as modems, email, networks, and telephones.
FIPPA	Means the BC *Freedom of Information and Protection of Privacy Act*, including all regulations and amendments.
Instant Messaging	A form of real time communication between two or more people based on typed text.

Formatted: Normal, Space Before: 0 pt

Formatted Table

Formatted: Font: 2 pt

Formatted: Header, Tab stops: 2.11 cm, Left

Formatted: Normal

Formatted: Font: +Body (Calibri), 11 pt

Formatted: Heading 1/O, Right: 0.27 cm, Space Before: 0.1 pt, After: 0.1 pt, Keep with next

Term	Definition
Misuse	Means any use of BC IT Resources in violation of this Policy, FIPPA or other applicable laws.
Monitoring	The collection and review of technical system data for the purpose of ensuring operational integrity, cyber security, and legal compliance. Monitoring does not imply unrestricted access to user content.
Non-BCIT Information	Means recorded information in the custody and control of BCIT that has not been collected, used, stored or disposed of for the purpose of BCIT business.
Personal Devices	Means user-owned devices, including laptops, tablets and other digital devices and equipment.
Personal Information	Means any recorded information about an identifiable individual, including without limitation, students, staff, researchers, research subjects, volunteers, and visitors, other than business contact information.
Personal Use Records	Means records that do not relate to BCIT business, programs or activities that a user creates, stores or maintains through IT Resources.
Privacy Risk Assessment (PIA)	Means an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 of the *Freedom of Information and Protection of Privacy Act*.
Privacy and Security Threshold Assessment (PSTA)	Means an assessment conducted by BCIT to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 of the *Freedom of Information and Protection of Privacy Act.*
Services	Includes but is not limited to email, file storage, portals, web page hosting and other web services, and other services.
Social Media Software	Any online application, platform, or tool that enables users to create and share content or participate in social networking. This includes, but is not limited to, platforms such as Facebook, X (formerly Twitter), Instagram, LinkedIn, and TikTok, as well as any internal social or collaborative tools.
User	A person who performs any action on an Information Asset.

Formatted: Normal, Space Before: 0 pt

INFORMATION SECURITY – POLICY #3502

REVISED DRAFT

BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

Cyber Security [draft revision]

Policy No:	3502
Version:	4
Category:	Information Management
Approving Body:	Board of Governors
Executive Sponsor:	VP Finance & Administration
Department Responsible:	Cyber Security Office
Directory of Records:	0650-15
Approval Date:	tbd / pending

Policy Statement

BCIT (the "Institute") maintains and protects the confidentiality, integrity, and availability of all information under its custody or control as required by applicable laws and regulatory requirements ("Cyber Security Framework"). This includes data stored, processed, and transmitted through BCIT's computing, communication, networking, and information technologies, and print data.

BCIT's Executive and the Board support the implementation of Cyber Security throughout the Institute.

Who This Policy Applies To

This policy applies to everyone who handles or makes decisions about information in BCIT's custody or control, including those connecting to BCIT information assets using personal equipment. It applies to all individuals, devices, and systems that access, manage, or interact with BCIT technology, including but not limited to:

- the Board of Governors;
- Faculty, Staff, and designated IT asset owners responsible for managing BCIT data and Information Technology/Operational Technology resources;
- students accessing BCIT systems, networks, and academic resources;
- researchers and research partners managing, storing, or transmitting research data;
- contractors, vendors, and third-party service providers with access to BCIT systems;
- alumni and visitors using guest networks or temporary access to BCIT resources;
- BCIT-Owned and Personal Devices such as laptops, desktops, and mobile devices used to connect to BCIT systems; and,
- Cloud and On-Premises Systems – BCIT-managed applications, databases, and cloud platforms.

Consequences of Policy Violation

Compliance with this Policy is mandatory for all users of BCIT's IT Resources. Users in breach of this Policy or engaging in Misuse will be subject to discipline, up to and inclusive of dismissal or expulsion. BCIT reserves the right to restrict, suspend, or withdraw access to BCIT systems and services, including computing privileges and network connectivity.

Investigations of suspected Misuse and any resulting actions will follow established Institute procedures and principles of fairness and due process.

In cases where Misuse or other user equipment or activity poses an immediate security or operational risk, BCIT may take temporary measures to protect Institute systems, such as disconnecting or quarantining affected devices, until the issue is investigated and resolved.

Person Device connecting to BCIT networks may also be subject to reasonable security restrictions to protect Institute systems and data integrity.

Purpose

This policy establishes the Cyber Security Framework ensuring the security and reliability of BCIT's information technology resources ("BCIT technology assets" or "information assets"). It requires that all users, devices, and IT environments adhere to cybersecurity best practices, regulatory compliance, and risk management protocols to protect the confidentiality, integrity, and availability of BCIT information assets.

Roles and Responsibilities

Roles	Duties and Responsibilities
BCIT Executive	The BCIT Executive is responsible for recommending an appropriate Information Security Framework to the Board of Governors, and for providing ongoing oversight of the Cyber Security Framework, including periodic independent reviews.
Chief Information Security Officer (CISO)	The CISO provides leadership and oversight for the security of BCIT's IT systems, data, and digital assets. Their responsibilities include developing and enforcing security policies, standards, ensuring compliance with applicable regulations and legislation, and maintaining a secure infrastructure capable of detecting, preventing, and responding to cyber threats. The CISO is the final authority for approving security exceptions.
Chief Financial Officer (CFO)	The CFO is responsible for reviewing requests to implement or operate electronic commerce systems or systems that store or process personal payment information, approving or denying such requests, and establishing any conditions that must be met.
Chief Information Officer (CIO)	The CIO provides strategic leadership and oversight for all aspects of enterprise technology at the Institute. This role encompasses shaping the overall technology strategy and fostering innovation to meet the evolving needs of BCIT community. The CIO is responsible for selecting, configuring, and supporting IT-issued devices, as well as providing communication tools such as email, messaging services, VOIP telephony, and audio/video conferencing.
Department Head / Dean (Business Owner)	Also referred to as Business owner. They are responsible for the oversight and governance of data within their academic or administrative unit. They act as the primary authority on how data

	should be classified, accessed, used, and protected, ensuring alignment with Institute cybersecurity policies and applicable laws such as the *Freedom of Information and Protection of Privacy Act* ("FIPPA" or the "Act") .
IT Administrators	Are responsible for the technical management and system configuration and implementation of required controls as per policy and standards (System Administrators, Database Administrators, Network Administrators, etc.).
IT Asset Owner	A designated individual or role responsible for ensuring that an IT asset is classified, properly used, protected, and maintained in accordance with BCIT's information security policies, standards, and procedures. This includes both physical and digital assets such as computers, servers, software, data, and network devices.
Director, Privacy, Information Access and Policy Management	The person responsible for overseeing and administering the process for completing and documenting Privacy Impact Assessments (PIAs) for all new systems, projects or programs, as required under the *Freedom of Information and Protection of Privacy Act* (FIPPA). A PIA is a risk management and compliance tool used to identify and address potential privacy and security risks. The Information Access and Privacy Office provides ongoing support to all Users to ensure that BCIT's use of Information Technology aligns with privacy protection requirements under FIPPA.
Director, Enterprise Risk & Internal Audit	The person responsible for identifying and assessing Institute risks, including those relating to the Cyber Security Framework.
End Users	Users must adhere to cybersecurity policy and report incidents promptly.
Third Parties	Contractors, vendors, and other external parties must comply with contractual and policy-related security requirements.

BCIT Commitment to Cyber Security Risk Management

BCIT is committed to a proactive and risk-informed approach to cybersecurity. This includes identifying, assessing, managing, and mitigating cybersecurity risks in alignment with institute objectives, regulatory requirements, and best practices. We strive to cultivate a culture of security awareness and shared responsibility across all levels of the organization. To uphold this commitment, BCIT will:

a) Establish and maintain a comprehensive cybersecurity risk management framework.
b) Continuously evaluate and strengthen controls that protect Institute digital infrastructure and sensitive information.
c) Regularly monitor the evolving threat landscape and adjust risk mitigation strategies accordingly.
d) Ensure cybersecurity roles, responsibilities, and accountability are clearly defined and understood across the Institute.
e) Promote collaboration between IT, academic, and administrative units to ensure

security is embedded in all processes and technologies.

f) Provide ongoing education, training, and resources to support cybersecurity awareness and readiness.

g) Conduct regular assessments and report cybersecurity risks, incidents, and mitigation progress to senior leadership and governance bodies.

By embedding cybersecurity risk management into BCIT's strategic and operational planning, we aim to safeguard our digital environment and support innovation, learning, and Institute resilience.

Cyber Security Framework Domains

1. Cyber Security Governance

The CISO is responsible for overseeing the implementation of cybersecurity policies and standards, including compliance and enforcement. Due to the dynamic nature of cyber threats, evolving regulatory landscapes, and our strategic objectives, policies and standards are not static. They are regularly reviewed and updated to maintain relevance, effectiveness, and adaptability.

A key element of the governance framework is the establishment of specialized Security Working groups. Among them, the SecOps ("Security Operations") Working Group plays a critical role in developing security standards. These standards then advance to the Cybersecurity Standards Committee for comprehensive review and endorsement, followed by final approval by the CISO. This multi-tiered approach ensures security standards are thoroughly vetted and refined before adoption.

2. Risk Management

BCIT is committed to proactively identifying, assessing, and managing cybersecurity risks by embedding risk management into decision-making processes, project lifecycles, and technology operations. All risks must be documented, evaluated, and addressed through mitigation, transfer, acceptance, or avoidance, in accordance with BCIT's risk appetite, risk tolerance, and compliance obligations. Risk assessments must be conducted regularly and in response to significant changes in systems, services, and emerging threats.

In compliance with FIPPA, a Privacy Impact Assessment (PIA) must be completed for all new initiatives. When sensitive personal information is disclosed or stored outside Canada, a Security Threat Risk Assessment (STRA) must also be conducted in collaboration with the Information Access and Privacy Office (IAPO). These assessments ensure that technical, legal, and operational risks are fully identified and appropriately mitigated. For detailed guidance, refer to the ***Cyber Security Risk Management Standard***.

3. Identity & Access Management (IAM)

BCIT must implement robust Identity and Access Management (IAM) practices to ensure that access to information systems and data is granted based on the principles of least

privilege, role-based access, and need-to-know. All user identities must be uniquely identifiable and authenticated before access is permitted. Access rights be regularly reviewed, promptly updated upon role changes or departures, and revoked when no longer required. All remote access to BCIT systems must be secured, authorized, and monitored to ensure the protection of Institute data and services. Multi-factor authentication (MFA) must be employed for systems containing BCIT sensitive or Personal Information. Systems that cannot meet current access requirements due to technical constraints should be treated as exceptions (see Policy Section 23). For detailed guidance, refer to the ***Identity and Access Management and Access Control Standard.***

4. IT Asset Management

BCIT must employ a systematic process for managing and tracking all IT assets to ensure that they are properly protected, maintained, and securely disposed of. Proper IT asset management allows the Institute to maintain control over its technological infrastructure, minimize security vulnerabilities, optimize asset utilization, and comply with applicable laws and regulations.

The IT Asset Management program will ensure that all information technology assets, hardware, software, and virtual/cloud resources, are accurately assigned owners, and are inventoried, tracked, and managed throughout their lifecycle.

4.1 System Categorization

Business Owners must classify all information systems based on sensitivity, business criticality, and potential impact. This classification will guide the application of security controls, risk management, and compliance measures. Critical or sensitive systems will have enhanced monitoring, incident response, and recovery protocols. In a security incident, system classification will determine response urgency, choice of procedures, and escalation to ensure effective mitigation, recovery, and communication. For a detailed guide, refer to the ***System Categorization and IT Asset Management Standard.***

5. Data Protection and Privacy

BCIT is dedicated to safeguarding the confidentiality, integrity, and availability of its information assets while upholding the privacy rights of individuals whose data it collects, processes, and stores. As a public institution, BCIT complies with FIPPA, governing the collection, use, disclosure, and protection of personal information. The institute ensures transparency and accountability in its operations and is committed to protecting the privacy of its staff, students, and the broader community.

To support this commitment, all Institute data must be classified based on its sensitivity, criticality, and applicable regulatory requirements. Information is categorized according to its potential impact on BCIT, its community, and external stakeholders if disclosed, altered, or lost. This classification framework enables risk-based decision-making, supports compliance with legal and regulatory obligations (such as FIPPA,, and PCI-DSS), and facilitates secure information sharing across academic, research, and administrative functions. All faculty, staff, students, contractors, and third-party service providers are

responsible for handling data appropriately, and ensuring safeguards are in place to prevent unauthorized access, use, disclosure, or destruction.

5.1 Information and Data Classification

BCIT implements a risk-based approach to information and data protection through formalized information and data classification, access control, retention, and secure disposal practices. Data should be securely managed throughout its lifecycle, including collection, storage, processing, transmission, and destruction.

Business Owners are accountable for classifying, protecting, and ensuring appropriate access to the data under their stewardship in accordance with BCIT cybersecurity and data governance policies. They must work with ITS and CSO teams to: apply appropriate safeguards based on the sensitivity and criticality of the data, manage data sharing, and respond to data-related risks or incidents. The following table outlines BCIT's information security classification:

Information Classification Levels	Description	Examples
PUBLIC INFORMATION		
PUBLIC - Applies to data and Information, that if compromised, would not result in injury to individual, or to BCIT or its partners	Information that is readily available to the public	• BCIT website • Brochures • Course descriptions • Published marketing information • Job postings
PROTECTED INFORMATION	Information that is restricted by a designated level of security and access control	
PROTECTED A – Applies to data and information that if compromised, could cause injury to an individual, or harm to BCIT and partners.	Information requiring a reasonable level of security controls with varying degrees of access control	• Administration procedures • Vendor or service provider • Departmental policies and procedures • Teaching materials
PROTECTED B – Applies to data and information that, if compromised, could cause serious injury to an individual, or serious harm to BCIT and its partners.	Information requiring the highest levels of security controls with varying degrees of access controls	• Research data and intellectual property • Drafts of strategic plans • Penetration testing reports • Locations of hazardous material storage
PROTECTED C – Applies to data and information that, if compromised, could cause grave injury to an individual or severe harm to BCIT and its partners	Information requiring the highest level of security controls with the highest degree of access control	• Social Insurance Numbers • Medical information • Financial information • Passwords and passphrases

5.2 Data Retention and Disposal

All BCIT data must be retained in accordance with applicable legal and regulatory obligations, and in compliance with BCIT Policy 6701-Records Management. Unauthorized deletion, alteration, or inappropriate storage of institutional data is prohibited. And data that is no longer required must be securely disposed of through approved data destruction methods as per the ***Secure Media Destruction Standard.***

5.3 Secure Transmission and Sharing of BCIT Electronic Data

BCIT will implement measures to ensure secure transmission and sharing of electronic information. All data, especially confidential information, must be transmitted using secure methods, including encryption and authenticated access, to prevent unauthorized access. Internal and external data sharing should occur through approved secure channels, and users must follow BCIT protocols. Data sharing is restricted to a need-to-know basis with documented authorization.

BCIT prohibits using insecure methods, such as unencrypted email or unauthorized file-sharing platforms, for sensitive data transmission. Users must adhere to secure communication practices, including strong authentication, encryption, and vigilance against phishing, malware, and social engineering. Unauthorized use, disclosure, or interception are prohibited and subject to disciplinary action. Refer to the ***Secure Transmission and Sharing of BCIT Electronic Information Standard.***

5.4 Payment Card Data Security

BCIT must comply with all applicable PCI DSS standards based on its merchant level. To ensure compliance, the following controls must be implemented:

i. **System Approva**l - Payment systems must be approved by the Chief Financial Officer before implementation.
ii. **Data Encryption** - Cardholder data must be encrypted during both transmission and storage.
iii. **Access Control** - Only authorized personnel may access payment systems, and all access must be monitored.
iv. **Fraud Prevention** - Systems must include safeguards to prevent fraud, unauthorized disclosure, and data manipulation.
v. **Third-Party Agreements** - External service providers that process payment card transactions or integrate with BCIT systems handling cardholder data must enter into binding agreements requiring full compliance with BCIT's cybersecurity policies and applicable PCI DSS requirements.
vi. **Secure System Design** - Systems must be designed to ensure confidentiality, integrity, and availability of payment information.
vii. **Vulnerability Scanning Compliance** - The Institute shall conduct regular internal and external vulnerability scans on systems that store, process, or transmit cardholder data, in accordance with PCI DSS requirements. These scans must be performed by qualified personnel or approved scanning vendors and documented for compliance validation.

6. Encryption

BCIT must employ the most current encryption mechanisms to protect sensitive data both in transit and at rest across all systems, networks, and devices, including removable media. Encryption must be implemented using current or higher industry-standard protocols and algorithms to prevent unauthorized disclosure, alteration, or destruction of Institute data. For more detailed guidance refer to the ***Encryption Requirement and Cryptographic Controls Standards***.

7. Network Security

To safeguard BCIT's IT and operational technology (OT) environments, comprehensive network security controls must be implemented. This includes enforcing strong access controls to defend against Advanced Persistent Threats (APTs), continuously monitoring all network segments for unauthorized access, anomalies, and potential cyber threats, and conducting security assessments or penetration testing following any significant network changes to identify and mitigate associated risks. For a detailed guide refer to the ***Network Security and Segmentation Standard.***

7.1 IP Address Assignment and Management

BCIT must maintain a centralized and secure system for managing all assigned Internet Protocol addresses (both IPv4 and IPv6) to ensure proper allocation, accountability, and protection of networked resources. All IP address assignments must be authorized and documented by the central IT department or designated authority. Unauthorized use or reallocation of IP addresses is prohibited. IP address management must support network segmentation, access control, incident response, and compliance with security monitoring and auditing requirements. For a detailed guide refer to the ***IP Address Management Standard.***

7.2 Domain Name Management

BCIT must maintain centralized oversight and control of all Institute domain names to ensure integrity, security, and alignment with official branding and communication standards. Registration, renewal, configuration, and Domain Name System management must be conducted by authorized personnel following established security practices, including secure registrar accounts, Domain Name System Security Extensions (where applicable), and change control procedures. Unauthorized registration or use of BCIT-affiliated domains is strictly prohibited. For a detailed guide refer to the ***Network Security and Segmentation Standard.***

8. Endpoint Security

BCIT must implement and enforce comprehensive endpoint security controls on all devices that access the institute information systems. This includes the use of standardized configurations, malware protection, device encryption, access control, and continuous monitoring to safeguard endpoints against evolving cyber threats. For a detailed guidance reference the ***System Security Hardening Standard*** and ***Vulnerability, and Patch Management Standard.***

9. Third-Party and Supply Chain Risk Management

BCIT must establish a structured Third-Party and Supply Chain Risk Management program to identify, assess, and manage cybersecurity risks associated with external entities. All third-party engagements must undergo thorough due diligence, incorporate defined security requirements within contracts, and be subject to continuous risk monitoring to safeguard Institute assets from unauthorized access, improper use, and operational disruptions.

BCIT may, on a case-by-case basis, host data or systems on behalf of third-party organizations, including affiliated non-profit entities. Where such arrangements exist, they should follow and adhere to the requirements outlined in the ***Third Party and Supply Chain Security Standard***.

10. User Awareness and Training

BCIT must establish and maintain an ongoing cybersecurity awareness and training program to ensure that all users (staff and students, contractors, and third-party vendors) understand their responsibilities in protecting BCIT's information and technology assets. All BCIT users should complete cybersecurity awareness training as part of onboarding and participate in refresher training at least annually or as needed based on emerging threats or regulatory changes. The Cybersecurity Office will periodically conduct phishing simulations to evaluate awareness.

11. Physical and Environmental Security

BCIT must implement and maintain comprehensive physical and environmental security controls to protect all sensitive areas, equipment, and assets from unauthorized access, damage, and disruption. These controls encompass both physical access limitations and environmental protections, helping to ensure protection of BCIT systems. Access to critical areas, including data centers, research and student labs, and administrative buildings, must be restricted to authorized personnel only. For more detailed guidance refer to the ***Data Center Physical Security Standard***.

12. Application Security

BCIT is committed to securing all applications throughout their lifecycle, including those developed internally, externally acquired, or created through industry-sponsored student projects. All applications must adhere to secure development practices to safeguard Institute data from unauthorized access, tampering, and service disruptions. No application may be deployed to production without a security review and CISO approval.

All application environments including, development, testing, staging, and production must be clearly segregated to prevent unauthorized access and cross-environment impact. Access must follow the principle of least privilege, granting users only the minimum necessary permissions based on their approved roles. All application security practices must align with recognized industry standards and frameworks to ensure consistent risk management across BCIT's digital ecosystem. For a detailed guide on Application Security, refer to the ***Secure Application Development and Modification Standard.***

13. Database Security

BCIT must enforce strong security controls across all Institute databases, relational and non-relational, to prevent unauthorized access, data tampering, and unplanned disruptions; ensuring data remains secure, accurate, and reliably accessible. All databases must adhere to recognized cybersecurity frameworks such as National Institute of Standards and Technology and Center for Internet Security, including access controls, encryption, vulnerability assessments, and audit logging.

Database administrators must enforce role-based access, restricted to authorized personnel and fully auditable. Databases containing sensitive or critical data require enhanced safeguards and regular security reviews. Security measures must be applied consistently throughout the database lifecycle, from design to deployment and ongoing management. For more detailed guidance refer to the ***Database Management Security Standard***.

14. Vulnerability and Patch Management

BCIT must implement and maintain a proactive vulnerability and patch management program across all IT, OT, and IoT environments to mitigate risks from known software and firmware weaknesses. Systems and applications must be regularly assessed, with vulnerabilities remediated based on risk severity and criticality.

Security patches must be applied promptly and in a controlled manner, following industry best practices and approved cybersecurity standards. Business units responsible for asset management must ensure periodic vulnerability scans and maintain auditable records of remediation or mitigation actions. Special attention must be given to systems handling sensitive BCIT data. For more detailed guidance, refer to the ***Vulnerability and Patch Management Standard.***

15. Change Management

BCIT must implement a formal change management process to ensure all changes to hardware, software, configurations, or procedures are reviewed, tested, approved, and documented to minimize risks to security, performance, and availability. All changes must be assessed for security impact prior to implementation. Changes must be authorized by the Change Advisory Board or designated approvers. Emergency changes must follow an expedited approval process and undergo a post-implementation review. Post-implementation monitoring is required to verify expected outcomes and ensure no adverse effects on security or performance.

16. Business Continuity Management

BCIT is committed to implementing and maintaining a Business Continuity Management program that ensures resilience against cyber threats and operational disruptions. All critical business functions and information systems must have documented, tested, and regularly updated continuity and recovery plans that align with BCIT 's risk tolerance and regulatory requirements. For more detailed guidance see also **Policy 7110, Emergency Management.**

17. Backup & Disaster Recovery

BCIT must implement effective backup and disaster recovery practices to safeguard critical data and IT infrastructure. Regular, secure backups and well-defined disaster recovery processes are essential to minimize operational downtime, prevent data loss, and maintain business continuity in the event of a disaster or cyber incident.

***17.1 Redundancy* & Infrastructure Resilience**

BCIT must design, implement, and maintain redundant and resilient infrastructure to minimize service disruptions from hardware failure, cyber-attacks, or natural

disasters. Infrastructure supporting mission-critical services must also include failover capabilities, and geographic distribution to ensure continuity and integrity. For more detailed guidance refer to the ***Backup and Recovery Management Standard.***

18. Incident Response & Monitoring

BCIT must maintain a formal Incident Response program to promptly identify, contain, investigate, and remediate cybersecurity incidents. All employees, contractors, and third-party partners must report suspected incidents immediately. Designated IR teams will follow documented procedures to minimize impact and prevent recurrence. Dedicated Incident Response Plans must be in place for both IT and OT environments. Regular cybersecurity tabletop exercises must be conducted to test response readiness and assess system resilience.

18.1 Incident Response & Activation

In the event of an incident (cyber related or disaster), the Cyber Security Incident Response Team (CSIRT) immediately assesses the situation and activates the appropriate IT Recovery Plan. A structured Incident Response Framework be used to contain, mitigate, and recover cyber threats or system failures. The CISO must test and maintain a detailed ***Cyber Security Incident Response Plan.***

18.2 Emergency Authority

If an emergency arises that threatens the security of Institute systems or data, the CISO has the authority and responsibility to implement emergency response measures to shut down the risk and to mitigate further damage. Those affected by such actions must be notified as soon as practicable. The CISO will immediately report any such emergency response measures to the BCIT Executive, and both will work to evaluate the risk and review next steps.

19. Cloud Security

BCIT must ensure the secure adoption and use of cloud services in alignment with its cybersecurity policies, standards, and applicable legal and regulatory obligations, including FIPPA. All cloud-based systems and data must follow principles of data classification, access control, encryption, and vendor risk management to safeguard Institute information and maintain accountability under a shared responsibility model.

Before implementation, cloud services must be assessed and approved by an appropriate BCIT governance committee or equivalent authority. Any service involving the collection, use, or disclosure of personal information requires a Privacy Impact Assessment (PIA) in accordance with FIPPA. If personal information is stored or processed outside of Canada, a Security Risk Assessment must also be conducted in collaboration with the Information Access and Privacy Office (IAPO) to identify and mitigate legal, technical, and operational risks. For more detailed guidance, reference the ***Cloud Security and Compliance Standard.***

20. Human Resources Security

Human Resource Security is critical to the protection of Institute information and IT systems. BCIT must ensure that all staff, contractors, and third-party vendors understand and fulfill their cybersecurity responsibilities. This includes ensuring proper screening, training, access control, and monitoring throughout the employee's life cycle.
Human Resource Security practices aim to minimize the risk of human errors, insider threats, or breaches resulting from personnel mishandling BCIT sensitive data or systems.

21. Email Security & Privacy

i. All electronic communications on BCIT systems must be safeguarded against unauthorized access, use, disclosure, or disposal through reasonable security measures.
ii. Users must transmit messages, attachments, and shared information securely using approved platforms. Sensitive or regulated data requires encryption and other protective controls.
iii. BCIT communication systems are subject to monitoring and auditing under Institute policies, applicable laws, and cybersecurity best practices. While privacy protections exist, communications may be accessed to ensure compliance and protect Institute integrity.
iv. Access to user email or electronic communications will occur only under authorized, lawful circumstances (e.g., investigations, operational continuity, legal obligations) with prior approval from designated authorities. Confidentiality and due process will be maintained.
v. Unauthorized use of personal email accounts for BCIT business is prohibited. Automatic forwarding of BCIT email (@bcit.ca) to non-BCIT accounts is not permitted. Refer to the **Secure Transmission and Sharing of BCIT Electronic Information Standard** for detailed guidance.

22. Compliance and Monitoring

BCIT must implement continuous compliance and monitoring practices to ensure adherence to institute cybersecurity policies, technical standards, regulatory requirements, applicable laws and industry approved standards. Systems, networks, and user activities may be monitored and audited regularly to detect violations, assess risk, and enforce security controls. All monitoring respects privacy laws and ethical guidelines while ensuring the integrity and security of BCIT information systems. For more detailed information refer to the ***Logging and Monitoring Standard.***

23. Exceptions

In exceptional circumstances where full compliance with cybersecurity policies is not feasible, a formal exception may be requested. All security policy exceptions must be documented, assessed for risk, and approved through BCIT's Cybersecurity Risk Management process, with final authorization by the CISO or their delegate. Approved exceptions must include compensating controls to mitigate associated risks and will be subject to periodic review, at least biannually or upon any significant system or operational changes.

APPENDICES

A. Technical Standards Associated with This Policy

Information Security Standards - https://authc.bcit.ca/it-services/secure/

B. Amendment History

		Approval Date	Status
1.	Creation: Policy 3502 version 1	2009 Jan 27	Replaced
2.	Revision: Policy 3502 version 2	2016 Oct 04	Replaced
3.	Revision: Policy 3502 version 3	2020 May 26	In Force
4.	Revision: Policy 3502 (draft) version 4	yyyy mm dd	Pending

C. Scheduled Review and Updates

This policy must be reviewed no later than five years from approval (next review date 2030 Dec 02 pending approval). However, it may be updated as needed to address emerging threats and changes in technology or regulatory requirements.

D. Definitions

Term	Definition
Asset Custodian	BCIT employee who has been assigned custody and control of an Information Asset.
Authentication	A process of verifying the identity of a user, system, or device before granting access to resources, applications, or services.
Authorization	The granting of permission in accordance with approved policies and procedures to perform a specified action on an Information Asset.
Business /Academic Head	The Dean, Director, or other person who has been assigned responsibility for a business unit.
Business Continuity	The Institute's ability to maintain or restore its business and academic services when some circumstance threatens or disrupts normal operations. (See Policy 7110, Emergency Management).
Business Owner	The BCIT employee who has been assigned responsibility for overseeing the lifecycle of one or more types of Information including responsibility for classifying and protecting Information.
BYOD	Refers to "bring your own device" and means a Mobile Device or Removable Media that is owned by the user.
Chief Information Officer (CIO)	BCIT Chief Information Officer.
Chief Information Security Officer (CISO)	BCIT Chief Information Security Officer.
Confidential Information	Any data or information that is meant to be kept private and secure, and whose unauthorized access, disclosure, or exposure could harm individuals or BCIT.
Contact Information	Means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business

	telephone numbers, business address, business email or business fax number of the individual.
Contractors	An individual or entity engaged under contract to perform specific work or services for BCIT, and who may require access to BCIT systems, facilities, or information assets during the course of their engagement.
CSO	Cyber Security Office.
Data	Data refers to raw, unprocessed facts, figures, or symbols that are collected, generated, or received by BCIT systems, individuals, or processes. Data may exist in digital, physical, or verbal form and becomes information when it is organized, interpreted, or contextualized to convey meaning.
Disaster Recovery	The activities that restore the Institute to an acceptable condition after suffering a disaster. See Policy 7110, Emergency Management for more information.
Encryption	The process of converting information or data into a coded format to make it unreadable, to prevent unauthorized access.
End Users	Individuals who interact with the system, application, or service on a daily basis. They are the final point of interaction in the technology chain and are usually not involved in the development or maintenance of the system.
ERM	BCIT Enterprise Risk Management
FIPPA	*Freedom of Information and Protection of Privacy Act* (BC)
Firewall	A system designed to prevent unauthorized access to or from a private network or between network zones.
GDPR	General Data Protection Regulation.
Information	Refers to all forms of institutional knowledge, data, and record, whether digital, physical, or verbal, that are created, stored, transmitted, or processed by BCIT. Information is considered an asset and must be protected against unauthorized access, disclosure, alteration, or destruction to preserve its confidentiality, integrity, and availability.
Information Security	The preservation of confidentiality, integrity, and availability of information. Confidentiality ensures that information is accessible only to authorized users. Integrity involves safeguarding the accuracy and completeness of information and processing methods. It may also include authenticity, auditability, accountability, non-repudiation, and reliability of information. Availability ensures that Authorized Users have access to IT assets when required.
Information Security Classifications	The information security categories are described in section 5.1 *Information Security Classifications.*
Information Technology (IT) Asset	Any device, system, software, application, data, or network component that is owned, leased, or managed by BCIT, or otherwise used to store, process, transmit, or secure institutional information. IT Assets include computing devices, servers, mobile equipment, cloud and network services, and digital information repositories that support BCIT's teaching, learning, research, and administrative operations.
IOT	Internet of Things

ITS	BCIT Information Technology Services.
Mobile Device	Includes any electronic device that is portable and contains Information, or has the ability to contain Information, or provides the ability to access or transmit Personal Information or Protected Information. Examples include laptops, tablet PCs, and any smart mobile devices.
OT	Operational Technology
PCI-DSS	Payment Card Industry Data Security Standard
Personal information	Means recorded information about an Identifiable Individual other than contact information
Removable Media	Information storage devices that are not fixed inside a computer. Examples include external hard drives, CD-ROMs, DVDs and USB flash drives.
Safeguard	A method of managing risk, including policies, procedures, practices, or BCIT structures, which can be of a physical, administrative, technical, management, or legal nature.
SCADA	Supervisory Control and Data Acquisition
Third-party service provider	An external organization engaged to deliver services on behalf of BCIT, which may involve access to, processing of, or storage of BCIT's data, systems, or networks.
Threat	Any potential event, action, or actor that could exploit a vulnerability to cause harm to a system, network, or BCIT.
Vendor	An external entity that supplies goods, technology, or software to BCIT, either through purchase, license, or subscription, and may have access to BCIT IT assets depending on the nature of the product or service and contract.
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more Threats.

E. Related Documents and Legislation

Law/Regulation/Policy	Document Name
BC legislation	*College and Institute Act*, RSBC 1996, c 52 *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 *Personal Information Protection Act*, SBC 2003, c 63
Federal legislation	*Criminal Code*, RSC 1985, c C-46 *Copyright Act*, RSC 1985, c C-42 Canada's Anti-Spam Legislation (i.e. CASL)[1]
Industry Standards	PCIDSS, Payment Card Industry Security Standards published by the Payment Card Industry Security Standards Council, including the "PCI Data Security Standard", the "PIN Transaction Security Requirements", and the "Payment Application Data Security Standard" NIST 800-82, (Guide to Industrial Control Systems Security) IEC 62443, (Industrial Automation and Control System Security) NERC CIP, (Critical Infrastructure Protection for energy systems) ISO 27001, (Information Security Management Systems)

	CIS Controls (Control 07: Continuous Vulnerability Management) NIST SP 800-40 Rev. 3, NIST SP 800-53, NIST SP 800-37 Rev. 2 CIS Controls v8 (Control 16: Application Software Security) NIST SP 800-218 (Secure Software Development Framework - SSDF) OWASP Top 10
BCIT Policies	1500, Code of Conduct 3501, Acceptable Use of Information Technology 5102, Student Code of Conduct (Non-Academic) 5900, Education Technology 6601, Intellectual Property 6700, Freedom of Information and Protection of Privacy 6701, Records Management 7506, Use of Materials Protected by Copyright 7170, Protection of Equipment and Property 7110, Emergency Management

INFORMATION SECURITY – POLICY #3502

REDLINE

BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

Policy

Information Security [draft revision]

Policy No:	3502
Version:	~~3~~4
Category:	Information Management
Approving Body:	Board of Governors
Executive Sponsor:	~~Chief Information Officer~~CFO and VP, Administration
Department Responsible:	~~Information Technology Services~~Cyber Security Office
Directory of Records Class:	0650-15
Approval Date:	~~2020 MAY 26~~tbd / pending

Policy Statement

BCIT ~~will take appropriate measures to preserve~~(the "Institute" maintains and ~~secure~~ protects the confidentiality, integrity, and availability of all information ~~in its custody and or~~ under its custody or control, ~~including all data stored in~~as required by applicable laws and regulatory requirements (Cyber Security Framework"). This includes data stored, processed, and transmitted through BCIT computing, communications, networking, and ~~other~~ information ~~technology resources~~technologies, and ~~including all data recorded in~~ print data~~or other fixed mediums; BCIT will protect all personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks~~.

BCIT's Executive and the Board support the implementation of Cyber Security throughout the Institute.

Formatted: Indent: Left: 0 cm

~~Purpose of Policy~~

~~The purpose of this policy is to:~~

Formatted: Indent: Left: 1.27 cm

- ~~Protect the confidentiality, integrity, and availability of all BCIT information~~
- ~~Ensure the integrity and security of BCIT information technology~~
- ~~Provide direction and support to management for information security in accordance with business requirements and applicable law~~
- ~~Define the roles of individuals and organizational entities involved in information security and establish the responsibilities of these roles~~
- ~~Ensure the reliable operation of BCIT's information technology so that all members of the BCIT community have access to the information assets they require~~
- ~~Ensure BCIT makes reasonable security arrangements to protect personal information in accordance with applicable law~~

Table of Contents

Who This Policy Applies To

This policy applies to everyone who handles or makes decisions about information in BCIT's custody or under BCIT's control, including those who use their own personal equipment to connectconnecting to BCIT information assets using personal equipment. It applies to all individuals, devices, and systems that access, manage, or interact with BCIT technology, including, but not limited to:

- the Board of Governors;
- Faculty, Staff, and designated IT asset owners responsible for managing BCIT data and Information Technology/Operational Technology resources;
- students accessing BCIT systems, networks, and academic resources;
- researchers and research partners managing, storing, or transmitting research data;
- contractors, vendors, and third-party service providers with access to BCIT systems;
- alumni and visitors using guest networks or temporary access to BCIT resources;
- BCIT-Owned and Personal Devices such as laptops, desktops, and mobile devices used to connect to BCIT systems; and,
- Cloud and On-Premises Systems – BCIT-managed applications, databases, and cloud platforms.

Related Documents and Legislation

Legislation
BC Statutes:
College and Institute Act, RSBC 1996, c 52
Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165
Personal Information Protection Act, SBC 2003, c 63

Federal Statutes:
Criminal Code, RSC 1985, c C-46
Copyright Act, RSC 1985, c C-42

- Canada's Anti-Spam Legislation (i.e. CASL)[1]

Industry Standards

Payment Card Industry Security Standards published by the Payment Card Industry Security Standards Council, including the "PCI Data Security Standard", the "PIN Transaction Security Requirements", and the "Payment Application Data Security Standard"

BCIT Policies

- 1500, Code of Conduct
- 1504, Standards of Conduct and Conflict/Interest Policy
- 3501, Acceptable Use of Information Technology
- 5102, Student Code of Conduct (Non-Academic)
- 6601, BCIT Intellectual Property Policy
- 6700, Freedom of Information and Protection of Privacy
- 6701, Records Management
- 7506, Use of Materials Protected by Copyright
- 7170, Protection of Equipment and Property
- 7110, Emergency Management

Definitions

Asset Custodian: means the BCIT employee who has been assigned custody and control of an Information Asset.

Authorization: means the granting of permission in accordance with approved policies and procedures to perform a specified action on an Information Asset.

Authorized User: means:

a) with respect to a set of Information, an individual who has been granted authority to access that set of Information by its Information Owner; and

b) with respect to an Information Asset, an individual who has been authorized to use that Information Asset by its Asset Custodian.

Business Continuity: means the Institute's ability to maintain or restore its business and academic services when some circumstance threatens or disrupts normal operations. It encompasses Disaster Recovery and includes activities such as assessing risk and business impact, prioritizing business processes, and restoring operations to a "new normal" after an event. See Policy 7110, Emergency Management for more information.

BYOD: refers to "bring your own device" and means a Mobile Device or Removable Media that is owned by the user.

Campus Security: means the BCIT Safety, Security and Emergency Management department.

Chief Information Officer (CIO): means the BCIT Chief Information Officer.

[1] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23

Contact Information: means information to enable an individual at a place of business to be contacted and includes the name, position name, or title, business telephone number, business address, business email or business fax number of the individual.

Disaster Recovery: means the activities that restore the Institute to an acceptable condition after suffering a disaster. See Policy 7110, Emergency Management for more information.

Encryption: means the process of obscuring information to make it unreadable without special knowledge.

External Party: means an organization or an individual who is not an employee or student who requires access to BCIT's Information Assets, excluding Public Assets, or BCIT Information, excluding Public Information.

Firewall: means a system designed to prevent unauthorized access to or from a private network or between network zones.

Head: means the Dean, Director, or other person who has been assigned responsibility for a business unit.

Inactive Account: means an account that has remained unused for the period of time specified in the Information Security Standard.

Information: includes all data and purported knowledge and facts in the custody or control of BCIT.

Information Asset: means equipment or systems controlled by BCIT that store, process, or transmit Information in electronic form; it does not include hardcopy record-keeping equipment or systems.

Information Owner: means the BCIT employee who has been assigned responsibility for overseeing the lifecycle of one or more sets of Information including responsibility for classifying and protecting Information according to the information security categories described in section 1.2 Information Security Classifications.

Information Processing Facilities: means any information processing system, service or infrastructure, or the physical locations housing them.

Information Security: means the preservation of confidentiality, integrity, and availability of information. Confidentiality ensures that information is accessible only to those authorized. Integrity involves safeguarding the accuracy and completeness of information and processing methods. It may also include authenticity, auditability, accountability, non-repudiation, and reliability of information. Availability ensures that Authorized Users have access to IT assets when required.

Information Security Classifications: means the information security categories described in section 1.2 Information Security Classifications.

Information Security Framework: means a comprehensive approach to Information Security that includes:

- Organizational structures with clearly defined roles and responsibilities
- Risk assessment and impact analysis
- Guiding principles
- Policies, procedures, and standards
- Controls and countermeasures

- Information Security awareness including education and training
- Ongoing monitoring of Information Security
- Resources such as financial and human resources required to implement the security framework
- Periodic reviews and assessment of the framework including, where appropriate, reviews by independent third parties

Information Security Incident: means an identified occurrence of a system, service, or network state indicating an actual, possible, or pending breach of Information Security or acceptable use policies, or a failure of Safeguards, or a previously unknown situation that may be security relevant.

Information Security Standard: means the set of technical standards published by the Cyber Security Officer from time to time, which is available online at https://www.bcit.ca/files/its/pdf/bcit_information_security_standards.pdf.

Inventory: means a complete list of all items in the category to which it refers that includes sufficient information to uniquely identify each item.

IT: means BCIT Information Technology Services.

IT Administrator: means the person responsible for configuring access to and monitoring access, usage, and performance of an Information Asset, including a system administrator, a network administrator, an application administrator, or a database administrator.

IT Service Management System: means BCIT's service request platform, which is accessible online at https://techhelp.bcit.ca.

Malicious Code: includes all code (including macros and scripts) that are deliberately coded to cause an unexpected or harmful event.

Mobile Device: includes any electronic device that is portable and contains Information, or has the ability to contain Information, or provides the ability to access or transmit Personal Information or Protected Information. Examples include laptops, tablet PCs, and any smart mobile devices.

Network Equipment: means any hardware or software, excluding workstations and servers unless configured to provide network services, that transmits or facilitates the transmission of Information, including switches, hubs, routers, bridges, Firewalls, modems, wireless access points, and DHCP, WINS, and DNS servers.

Personal Information: means recorded Information about an identifiable individual other than contact information.

Privacy Office: means the BCIT Information Access and Privacy Office.

Protected Information: means Information and Information Assets that are designated as "Protected" under Section 1.2 Information Security Classifications. Protected Information is categorized as Protected A, Protected B or Protected C and is marked accordingly.

Public Asset: means an Information Asset that has been designated as available to members of the public. Examples include kiosks and the public website.

Public Information: means information categorized as "Public" under section 1.2 Information Security Classifications. Public information is readily available to any member of the BCIT community or to the general public either upon request or by virtue of being posted or published by BCIT.

Record: has the same meaning as the definition of "Records" in Policy 6701, Records Management.

Removable Media: means Information storage devices that are not fixed inside a computer. Examples include external hard drives, CD-ROMs, DVDs and USB flash drives.

Safeguard: means a method of managing risk, including policies, procedures, practices, or organizational structures, which can be of physical, administrative, technical, management, or legal nature.

Threat: means a potential cause of an unwanted Information Security Incident, which may result in harm to a system or organization.

Vulnerability: means a weakness of an asset or group of assets that can be exploited by one or more Threats.

Duties and Responsibilities

BCIT Commitment to Information Security

The Board of Governors and BCIT Executive actively support Information Security within the organization.

Board of Governors

The BCIT Board of Governors is responsible for establishing an Information Security Framework for the Institute.

BCIT Executive

The BCIT Executive is responsible for recommending an appropriate Information Security Framework to the Board of Governors, and for providing ongoing executive oversight of the Information Security Framework, including periodic independent reviews.

Chief Financial Officer

The Chief Financial Officer is responsible for reviewing requests to implement or operate electronic commerce systems or systems that store or process personal payment information, approving or denying such requests, and establishing any necessary conditions that must be met.

Cyber Security Officer

The Cyber Security Officer provides leadership and oversight over all aspects of cyber security, including cyber threat and risk management, developing and delivering an institutional cyber awareness program, security policies, procedures and standards formation and application. The Cyber Security Officer publishes and maintains the Information Security Standard and reviews it periodically in light of changing expectations and risks.

Director, Enterprise Technology

The Director, Enterprise Technology provides leadership and guidance in all aspects of

enterprise technology. Drives technology strategy and innovation on behalf of the Institute. Accountable for the effective and efficient management and delivery of IT infrastructure, application development, systems integration, architecture and operations.

BCIT Management

Members of BCIT Management are responsible for ensuring that employees and others under their supervision are aware of their Information Security responsibilities.

Privacy Office

The Privacy Office is responsible for:

- BCIT's privacy management framework
- Oversight of compliance with applicable privacy laws and regulations
- Privacy impact assessments covering data impact and vendor assessments
- Privacy breach response and regulatory reporting

Director, Enterprise Risk

The Director, Enterprise Risk is responsible for identifying and assessing overall risk for BCIT.

Policy Details

1. Asset Management

1.1 Custody and Use of Assets

1.1.1 Information Asset Assignment and Transfer of Custody

a) Every business unit must assign an Asset Custodian to each Information Asset in the business unit's custody.

b) If an Asset Custodian who has been assigned to an Information Asset is no longer assigned to a business unit, the business unit must assign a new Asset Custodian to each Information Asset that was assigned to the departing Asset Custodian, and must ensure that custody of each Information Asset is transferred to the new Asset Custodian.

1.1.2 Information Asset Inventory

Every business unit must maintain a current Inventory of all Information Assets in the business units' custody. The Inventory must include the name of the current Asset Custodian for each asset, and also the location of the asset (as long as the asset is not a Mobile Device).

Refer to Procedure 3502-PR1, Information Security.

1.1.3 Information Asset Location

Every Asset Custodian must provide the location of all Information Assets assigned to them upon request from the Asset Custodian's business unit.

1.1.4 Acceptable Use of Assets

Every Asset Custodian must ensure that every Information Asset in their custody is used and operated in accordance with Policy 3501, Acceptable Use of Information Technology.

1.2 Information Security Classifications

Information classification in the context of Information Security is the classification of Information based on its level of sensitivity and the impact to BCIT if the information was disclosed, altered or destroyed without authorization. The classification of Information helps to determine the appropriate security controls for safeguarding the information.

When Information and Information Assets are classified for the purpose of applying an appropriate level of Information Security and controls for handling a set of Information, BCIT employees must use the Information Security Classifications in this section:

Category and Scope of Information	Description
PUBLIC INFORMATION	
PUBLIC – Applies to data and Information that, if compromised, would not result in injury to individuals, or to BCIT or its partners.	Information that is readily available to the public.
PROTECTED INFORMATION	Information that is restricted by a designated level of security and access control.
PROTECTED A - Applies to data and Information that, if compromised, could cause injury to an individual, or harm to BCIT and its partners.	Information that requires a reasonable level of security controls with varying degrees of access control.
PROTECTED B - Applies to data and Information that, if compromised, could cause serious injury to an individual, or serious harm to BCIT and its partners.	Information that requires the highest level of security controls with varying degrees of access control.
PROTECTED C – Applies to data and Information that, if compromised, could cause grave injury to an individual or severe harm to BCIT and its partners.	Information that requires the highest level of security controls with the highest degree of access controls.

Formatted: Font: Not Bold

Formatted: Space Before: 0 pt, After: 0 pt, Widow/Orphan control, Don't keep with next, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

1.2.1 Information Ownership

Every business unit must assign an Information Owner to each set of Information in the business unit's custody or control.

For further details about establishing Information Ownership, see Procedure 3502-PR1, Information Security.

1.2.2 Classifying Information

a) Every Information Owner must classify each set of Information assigned to them according to the Information Security Classifications. Where applicable, Information Owners should collaborate with the Privacy Office to classify and manage the Information for which they are responsible.

b) Information should be classified based on an evaluation of its value, sensitivity, intended use, and other relevant factors

according to the categories in Information Security Classifications. Information may be classified at a higher level of Information Security but not at a lower level of security. Information Assets that store Protected Information are to be assigned an Information Security Classification at the highest protection or classification of the Information it contains.

c) Reclassifying Information: If Information changes, or if more than 18 months have passed since that set of Information was last classified or reviewed for classification, the Information Owner must reevaluate the assigned classification to ensure it is still appropriate and, if applicable, reclassify the Information according to the Information Security Classifications.

1.2.3 Marking Protected Information

a) every Information Owner must mark each set of Information assigned to them that is designated as Protected Information according the Information Security Classifications.

b) Information security markings for Protected Information must be in eye-readable form. Reproductions of Protected Information must be marked in the same manner as the originals.

1.2.4 Electronic Storage

Where possible, marking of Protected Information for electronic storage material should be both in eye-readable and machine-readable form.

1.3 Information Handling

1.3.1 Information Handling, Accuracy, and Reproduction

a) Every Authorized User of a set of Information must carry out all tasks related to the creation, storage, maintenance, classification, use, disclosure, , and disposal of the Information responsibly, in a timely manner, and with the utmost care.

b) Authorized Users must take all reasonable steps to ensure the accuracy of all Information that they create or modify.

c) Authorized Users must not reproduce Protected Information unless they are authorized by the Information Owner to do so.

1.3.2 Information Sharing

a) Authorized Users may disclose Protected Information to other Authorized Users of that Information on a need-to-know basis for the performance of their duties but otherwise must not disclose such Information unless they are authorized by the Information Owner to do so.

b) Employees must only seek to access and use the minimum Protected Information necessary for the performance of their duties.

c) Authorized Users may only collect, use, or disclose Personal Information in accordance with Policy 6700, Freedom of Information and Protection of Privacy.

1.3.3 Sharing Information or Information Assets with External Parties

a) An Information Owner may not authorize an External Party to be an Authorized User of Information unless the Information Owner has ensured that:

i. an analysis has been conducted of the foreseeable risks to BCIT arising from access of the Information by the External Party;

ii. any identified risks have been suitably mitigated through appropriate Safeguards; and

iii. the External Party has entered into a suitable contract with BCIT by which they are legally required to comply with all BCIT policies that apply to the Information.

1.3.4 Encryption of Protected Information

Every Information Owner must ensure that all sets of Information assigned to them that are designated as Protected Information are encrypted in accordance with the Information Security Standard, regardless of whether the Information is stored in an Information Asset or hardcopy. This includes data outside of BCIT stored in a cloud service, and/or held on a Mobile Device.

1.3.5 Printing of Protected Information

No one may send Information designated as Protected Information to a shared printer unless they use a passcode to release the hardcopy of the Information to their sole custody at the printer, or an Authorized User of the Information is present at the printer to receive the hardcopy as it is printed.

1.3.6 Handling and Safeguarding of Personal Information

Every Information Owner must ensure that where sets of Information assigned to them include Personal Information, that the Information is handled in accordance with Policy 6700, Freedom of Information and Protection of Privacy.

1.3.7 Deleting Information Created or Owned by Others

Every Information owner must, for each set of Information assigned to them:

iv. establish protocols consistent with Policy 6701, Records Management that set out how the Information may be deleted; and

v. ensure the Information is protected against unauthorized or accidental changes.

2. Physical and Environmental Security

2.1 Securing Premises

2.1.1 Physical Security Perimeter

a) Subject to paragraph (b) below, business units must establish physical Safeguards to protect areas that contain Information Assets or hardcopy that contains Protected Information, or Personal Information, including security perimeters, such as walls, with well-defined access points, such as card-controlled entry. The level of protection provided by the physical Safeguards must be commensurate with identified risks.

b) Paragraph (a) does not apply to Mobile Devices and Removable Media on which the Information is encrypted in accordance with sections 3.4 and 3.7.2, respectively.

2.1.2 Physical Entry Controls

Business units must ensure that areas requiring higher levels of security are protected with appropriate entry Safeguards that restrict access to Information to Authorized Users.

2.2 Equipment Security

2.2.1 Equipment Siting and Protection

Business units must ensure that sites chosen as locations for Information Assets or hardcopy that store Information are suitably protected from physical intrusion, temperature fluctuations, theft, fire, flood, and other hazards.

2.2.2 Physical Security of Equipment

a) Asset Custodians must ensure the physical security of their assigned Information Assets, regardless of whether the asset is located on or off BCIT campuses.

b) Asset Custodians may delegate the responsibility described in paragraph (a) within their business unit.

2.2.3 Use of Equipment On-Campus

a) No one may use an Information Asset unless they are an Authorized User.

b) Asset Custodians must ensure their assigned Information Assets are only used by Authorized Users.

c) A member of the public is deemed to be an Authorized User of a Public Asset if they comply with all conditions of access established by the Asset Custodian.

2.2.4 Supporting Utilities

Business units must ensure that Information Assets are protected

from power failures and other disruptions caused by failures in supporting utilities.

2.2.5 Cabling Security

Business units must ensure that:

i. Information Assets consisting of cables, wires, or other equipment that transmits Information or supports Information services are protected from interception or damage; and

ii. utilities that support Information Assets, such as power and cooling lines, are suitably protected from damage.

2.2.6 Equipment Maintenance

Business units must ensure that Information Assets and supporting equipment are properly maintained to ensure their continued availability and integrity.

2.2.7 Security of Equipment Off Campus

a) Authorized Users of Mobile Devices and Removable Media may take these Information Assets off of BCIT campuses if the Authorized User complies with all conditions established by the Asset Custodian.

b) Information Assets that are not Mobile Devices or Removable Media may not be taken off of BCIT campuses unless the individual doing so:

i. is an Authorized User;

ii. has received prior written authorization from the Asset Custodian that expressly permits the asset to be removed from BCIT campuses; and

iii. complies with all conditions established by the Asset Custodian.

c) An Authorized User who takes an Information Asset off of a BCIT campus must:

i. Notify the Asset Custodian that the asset is being taken off of campus; and

ii. Ensure the security of the asset at all times.

2.2.8 Secure Disposal or Re-use of Equipment

Business units may not dispose of Information Assets or recondition Information Assets for reuse unless the Asset Custodian has:

i. ensured that all Information stored in the asset has been rendered unrecoverable;

ii. ensured that all foreseeable security risks have been mitigated; and

iii. authorized the person who will be carrying out the disposal or reconditioning to do so.

2.2.9 Loss or Theft of Assets

a) Any person who has knowledge of a loss or theft of an Information Asset or a hardcopy record containing Information, or who believes such loss or theft has occurred, must immediately report their knowledge and belief to Campus Security, and the appropriate Information Owner and business unit to which the asset or hardcopy record is assigned.

b) If there is a risk that Protected Information may be accessed by someone who is not an Authorized User then Campus Security must immediately inform the Cyber Security Officer and the Privacy Office of the risk and provide relevant details.

c) If the asset is a Mobile Device that is likely to contain Protected Information, the person reporting on a loss or theft must report this to Campus Security, the Cyber Security Officer, and the Privacy Office.

d) Campus Security must conduct an initial assessment and prepare an incident report. Campus Security must inform the Cyber Security Officer and the Privacy Office and provide copies of the incident report.

3. Management of Information Systems and Devices

3.1 Operational Procedures and Responsibilities

3.1.1 Documented Operating Procedures

Business units must establish operating procedures for their assigned Information Assets, and must document, maintain, and make the procedures available to all Authorized Users.

3.1.2 Change Management

Business units must control changes to Information Processing Facilities and related systems through appropriate change control mechanisms.

3.1.3 Segregation of Duties

Business units must segregate duties and areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of Information Assets and Information.

3.1.4 Separation of Development, Test, and Operational Facilities

Business units must separate development, test, and operational facilities and systems to reduce the risks of unauthorized access or changes.

3.2 External Party Service Delivery Management

Business units must, for all Information and Information Assets assigned to them:

i. ensure that all contractual relationships with External Parties incorporate all applicable BCIT security policies as legally binding obligations on the External Parties; and

ii. monitor compliance of External Parties with the applicable security requirements throughout the entire period that the Information or Information Asset is accessible by the External Party.

3.3 System Planning and Acceptance

Prior to accepting new Information systems, upgrades, or versions, business units must:

i. conduct suitable tests of the system during the development phase;

ii. established suitable acceptance criteria; and

iii. ensure the new system satisfies the acceptance criteria.

3.4 Mobile Devices

a) Business units may only issue Mobile Devices to Authorized Users.

b) Business units must ensure all Information on a Mobile Device is suitably encrypted and protected from unauthorized access at all times with a combination of a PIN, password or lock at the device level.

c) Authorized Users may only use Mobile Devices for the purpose for which they are issued.

d) Authorized Users must not permit anyone else to access a Mobile Device assigned to them.

e) Authorized Users of Information who are permitted to access the Information with a BYOD must comply with Procedure 3502-PR1, Information Security Procedure, section 4, Mobile Device Security. See also section 1.3, Information Handling, above, and the Information Security Standard.

3.5 Protection against Malicious Attacks

Authorized Users must carefully evaluate websites and emails when clicking/downloading links and take reasonable precautions to avoid spyware traps and phishing sites.

3.5.1 Training & Awareness

a) The Cyber Security Officer must minimize risks to the Institute's systems and Information from Malicious Code by fostering employee awareness, encouraging employee vigilance, and deploying appropriate protective systems and devices.

b) IT Administrators must inform all relevant business units and

individuals of Threats and appropriate Safeguards they can take to protect the Institute's systems and information.

c) Business units and Authorized Users must stay informed about Threats and appropriate Safeguards and must take reasonable precautions in using Information Assets and hardcopy and in accessing Information in order to minimize opportunities for attacks.

3.5.2 Anti-Virus

a) Authorized Users must always run Institute standard anti-virus software with a continuous update cycle.

a) Authorized Users must install all operating system patches (Windows, Apple, and Linux) as soon as they become available.

3.5.3 Backup

a) System owners must establish the extent, frequency, and retention of system backups in accordance with the business requirements of the Institute, the security requirements of the Information involved, and the criticality of the Information to the continued operation of the Institute.

b) IT Administrators must configure their Information Assets to meet the backup requirements.

See also Procedure 3502-PR1, Information Security Procedures.

3.5.4 Backups must be Secured and Tested

IT Administrators must:

i. secure backups in accordance with the classification of the Information they contain;

ii. periodically test backups to ensure the Information is recoverable; and

iii. keep Records of conducted tests.

3.5.5 Backups must not be used in lieu of other controls

Business units must not rely on backups to replace Records management Safeguards or to provide audit trails.

3.5.6 Recovering and Restoring Information

Business units must ensure Safeguards are in place to protect the integrity of Information when recovering and restoring Information, especially where restored files may replace more recent files.

3.6 Network Security Management

a) IT Administrators must ensure:

i. their networks are adequately managed and Safeguarded in order to be protected from Threats,

and in order to maintain security for the systems and applications using the networks, including Information in transit; and

ii. all equipment connected to their networks complies with all applicable BCIT policies.

b) Authorized Users of a BYOD may only connect the BYOD to a BCIT network if:

i. the IT Administrator has inspected the BYOD prior to connection to verify that security requirements are met; and

ii. the Authorized User permits the IT Administrator to inspect the BYOD and verify its compliance on an ongoing basis.

3.6.1 Network Controls

a) IT Administrators must establish special Safeguards to:

i. ensure the confidentiality and integrity of data passing over public networks or over wireless networks;

ii. protect Network Equipment, the connected systems, and applications; and

iii. maintain the availability of the network services and connected computers.

b) IT Administrators must implement appropriate logging and monitoring to ensure a Record is created for all security relevant actions.

3.6.2 User Authentication for External Connections

a) IT Administrators must establish suitable remote access Safeguard protocols that include robust identification, authentication, and Encryption techniques.

b) No one may access BCIT networks remotely unless they do so with technology approved by the BCIT Director of Enterprise Technology and comply with all applicable BCIT policies.

3.6.3 Use of non-BCIT Systems for BCIT business

a) Subject to paragraph (b) below, anyone conducting BCIT business using systems other than BCIT owned systems must do so in accordance with the Information Security Standard.

b) Academic and administrative business units may deviate from the Information Security Standard if:

i. the business unit receives an exemption from the Chief Information Officer pursuant to a request made through the IT Service Management System; and

ii. the business unit complies with all conditions established in the exemption.

3.6.4 Remote Configuration and Diagnostic Port Protection

IT Administrators must implement suitable Safeguards to secure physical and logical access to configuration and diagnostic ports.

3.6.5 Segregation in Networks

a) IT Administrators must ensure network isolation and segregation is practiced as part of enterprise architecture that:

i. is compartmentalized to prevent intrusion into, or interference with, BCIT systems or other networks;

ii. has redundancy, backup and recovery measures, and contingency plans in place that ensure network services are available on a sufficiently timely basis to support the intended uses; and

iii. has documentation covering its topology, configuration, and gateways to external networks and nodes, as well as the connected devices and individuals responsible.

b) IT Administrators must ensure that Information Assets are not attached to two networks simultaneously, except for Network Equipment approved by the IT Administrator for such simultaneous attachment.

3.6.6 Network Connection Control

a) No one may connect Network Equipment to BCIT networks unless they have approval from IT and comply with any conditions in the approval.

b) IT Administrators must ensure systems and equipment connected to the BCIT network are configured to minimize the possibility of bypassing access Safeguards.

See the Information Security Standard for configuration details.

3.6.7 IP Address Assignment

a) Subject to paragraph (b) below, IT Administrators must ensure that no one assigns or uses IP addresses on BCIT networks unless IT has given permission for such assignment or use.

b) Automated assignment of an IP address by an IT controlled DHCP server constitutes permission of IT.

3.6.8 Domain Name Registration and Use

a) IT Administrators must ensure that no one registers domain names that include "BCIT", "British Columbia Institute of Technology", or similar unless BCIT's Marketing and Communications Department has given prior Authorization to do so.

b) IT Administrators must ensure that agreements with External Parties include protection for BCIT domain names. See section 1.3.3, Sharing Institute Information or Assets with External Parties.

c) IT Administrators must ensure all websites that are sub-domains of a BCIT domain or assigned to a BCIT owned IP range are authorized by BCIT's Marketing and Communications Department prior to development.

3.6.9 Server Placement in Networks

a) IT Administrators must ensure:

i. servers that are connected to the BCIT network are situated in a location and network zone with logical and physical security that is commensurate with the value of the service provided and the sensitivity of the Information accessible through the system; and

ii. all access to the servers described in paragraph (a) is logged to facilitate auditing.

See the Information Security Standard for minimum logging standards.

b) IT Administrators must ensure student servers are only connected to and able to access the student network and are not attached to any other network such as research or administration.

3.6.10 Servers Accessible from External Networks

IT Administrators must ensure no servers are accessible by an external network, including the Internet, unless the Cyber Security Officer has given permission for such access.

3.6.11 Security of Network Services

IT Administrators must ensure that security features, service levels, and management requirements for each network are identified and included in any service level agreement, regardless of whether these services are provided in-house or outsourced.

3.7 Handling of Media and Hardcopy

3.7.1 Media and Hardcopy Handling Procedures

Information Owners must:

i. create protocols consistent with the Information Security Standard for handling, processing, storing, transporting, transmitting, and disposing or reusing media and hardcopy that contains Information assigned to them; and

ii. ensure such protocols are complied with.

For details, see the Information Security Standard.

3.7.2 Encryption of Information on Removable Media

Information Owners must ensure that all of their assigned sets of Information designated as Protected Information that are stored on Removable Media are Encrypted in accordance with the Information Security Standard.

3.7.3 Disposal or Reuse of Media

Asset Custodians must ensure that prior to disposal or reuse of any of their assigned media that it is impossible to recover any Information previously stored on the media.

3.7.4 Shredding of Unwanted Hardcopy Records

Information Owners must ensure that all hardcopy records designated as Protected Information are securely shredded when the Information is no longer required, and that the requirements of procedure 6701 PR1, Records Management Procedure are satisfied for Information that is contained in a Record.

3.7.5 Using External Service Providers

Information Owners must ensure that there is an agreement in place with any External Party used for storage and disposal of media and hardcopy records that includes binding obligations to comply with all applicable BCIT policies, including section 1.3.2, Sharing Information or Information Assets with External Parties.

3.7.6 Security of System Documentation

IT Administrators must ensure that system documentation is protected against unauthorized access.

3.8 Exchange of Information

3.8.1 Information Exchange Policies and Procedures

Information Owners must ensure that formal Information exchange policies, procedures, and Safeguards are in place to protect the exchange of Information through the use of all types of communication.

3.8.2 Transmission and Sharing of BCIT Electronic Information

a) Information Owners must ensure that all Information designated as Protected Information is Encrypted in transit, including by email, electronic data interchange, and other forms of interconnection of business systems.

b) Information Owners must ensure that Safeguards are in place to verify the integrity of transmitted Protected Information and the identities of sender and receiver.

c) No one may enable automatic forwarding or redirecting of BCIT business email account (@bcit.ca) to a non-BCIT account such as personal email account (Gmail, Yahoo).

3.8.3 Persons Giving Information over the Telephone

Information Owners must ensure the identity and Authorization of callers is verified before Protected Information is disclosed to them

through audio communications such as telephones.

3.8.4 Exchange Agreements

Information Owners must ensure:

i. suitable agreements are established with External Parties prior to disclosure of Protected Information to them; and

ii. the disclosure of Personal Information to External Parties complies with Policy 6700, Freedom of Information and Protection of Privacy.

3.8.5 Removable Media in Transit

Asset Custodians must ensure Removable Media containing Information is protected against unauthorized access, misuse or corruption during transportation using a suitable standard of Encryption.

See the Information Security Standard.

3.9 Electronic Commerce Services

a) Business units must establish such additional Safeguards as are appropriate to cover the additional security requirements associated with using or providing electronic commerce services.

b) Business units must ensure:

i. Information involved in electronic commerce is protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification; and

ii. electronic commerce systems comply with all applicable Payment Card Industry (PCI) standards.

3.9.1 Approval of Electronic Commerce Systems

No business unit may implement or operate an electronic commerce system unless it has been approved by BCIT's Chief Financial Officer prior to implementation and the business unit complies with any conditions established by the Chief Financial Officer.

3.9.2 Personal Payment Information

No business unit may implement or operate a system that stores or processes personal payment Information, including credit card numbers and bank account numbers, unless it has been approved by BCIT's Chief Financial Officer prior to implementation and the business unit complies with any conditions established by the Chief Financial Officer.

3.10 Monitoring

3.10.1 Logging

Information Owners must produce logs recording security relevant

user activities, exceptions, and Information Security events, and must keep such logs for the period specified in the Information Security Standard for access control monitoring.

3.10.2 Monitoring System Use

Information Owners must monitor logs, including system and application logs, and must investigate any anomalies.

IT Administrators must regularly review logs for security events by IT and must report discrepancies to the Cyber Security Officer.

3.10.3 Protection of Log Information

Information Owners must ensure logging facilities and log Information are protected against tampering and unauthorized access.

3.10.4 Administrator and Operator Logs

IT Administrators must ensure that administrator and other privileged account activities are logged.

3.10.5 Clock Synchronization

a) IT Administrators must ensure system clocks are regularly synchronized to a common source to simplify the review and correlation of audit logs.

b) IT must specify the common source.

4. Identity and Access Management

System owners may provision accounts in accordance with this section to provide access to Information Assets including networks, operating systems, applications, and database management systems.

4.1 Access Control Policy

System owners must establish, document, and regularly review an access control policy for systems in their control based on business and security requirements for access. Access must be based on the principle of least privilege and need-to-know basis.

4.2 User Access Management

a) System owners must ensure formal user registration and de-registration procedures are used to grant and revoke access to all Information systems and services including network services, operating systems, applications, and database management systems.

b) System owners must ensure:

i. the allocation and use of privileges is restricted and controlled; and

ii. the allocation of passwords and other security credentials is controlled through a formal management process.

4.2.1 Review of Accounts and Access Rights

System owners must review users' access rights at regular intervals using a formal process.

4.2.2 Removal of Access Rights

System owners must ensure that for employees who are leaving employment, all employee-based access is disabled at the end of the employee's last day, or sooner, based on security requirements.

4.2.3 Session Time-out

System owners must ensure inactive sessions are terminated after the period of inactivity described in the Information Security Standard.

4.2.4 Additional Access Protections

System owners must ensure that any other appropriate access protections based on time of day, location, or additional authentication requirements are implemented and maintained.

4.3 Additional User and Business Unit Responsibilities

4.3.1 Authentication

Authorized Users must authenticate their account using approved login procedures prior to accessing a system.

4.3.2 Delegation of Duties

Authorized Users may only delegate duties by:

i. employing features within the system where the system permits; or

ii. through the controlled sharing procedure for delegating an account set out in Procedure 3502-PR1, Information Security Procedures.

4.3.3 Short Term Accounts

Business units that employ temporary employees on a frequent basis using short term accounts must follow Procedure 3502-PR1, Information Security Procedures.

4.3.4 Inadvertent Access to Resources and Information

a) Authorized Users must not:

i. exploit insecure accounts or resources;

ii. take advantage of less knowledgeable users; or

iii. access Information without Authorization.

b) Authorized Users must immediately report any Information Security Incidents to IT.

4.3.5 Password Use

a) Authorized Users must:

i. follow good security practices (strong & complex password paraphrase) in the selection and use of

passwords; and

ii. comply with the procedures relating to passwords in Procedure 3502-PR1, Information Security Procedures.

b) Authorized Users must not:

i. disclose their passwords to anyone, except for Authorized Users who are delegating an account according to Procedure 3502-PR1, Information Security Procedures; or

ii. use their BCIT passwords for any non-BCIT accounts or services (such as personal ISP email accounts, instant messaging accounts, social media sites, or other online services).

4.3.6 Controlling Access to Unattended User Equipment

a) Authorized Users must not leave an Information Asset unattended unless they:

i. log off or use device locking software; and

ii. prevent theft of the asset by using a locking device.

b) Business units must ensure that all unattended Information Assets in public areas are physically secured and configured in a manner such that the asset and any Information it contains are secure.

4.3.7 Controlling Access to Information in Unattended Areas

Authorized Users must secure hardcopies containing Personal Information or Protected Information from unauthorized access.

5. Information Systems Procurement, Development & Maintenance

5.1 Security Requirements of Information Systems

a) System owners must ensure security controls are specified for all business and contract requirements as well as for new Information systems, or enhancements to existing Information systems including off-the-shelf and custom-built software.

b) System owners must ensure system requirements for Information Security and processes for implementing security are integrated in the early stages of Information system projects.

For requirements that must be considered, see the Information Security Standard.

5.2 Correct Processing in Applications

System owners must ensure that the systems for which they are responsible handle Information with due care, including validation of Information entered into the system, validation checks to detect corruption of Information through processing errors or deliberate acts, appropriate controls to ensure authenticity and message integrity, and

validation of Information output from an application to ensure that the processing of stored Information is correct.

5.3 Security in Development, Deployment and Support Processes

a) No one may access operational software libraries or the source code of systems except Authorized Users.

b) IT Administrators must ensure that segregation of duties, technical access controls, and robust procedures are employed whenever amendments to software are necessary.

5.3.1 Technical Review of Applications after Execution Environment Changes

IT Administrators must ensure that when the execution environment of the application is changed (e.g., operating system, hardware, middleware), that business critical applications are reviewed and tested to ensure there is no adverse impact on Institute operations or security.

5.3.2 Outsourced Software Development

IT Administrators must ensure that outsourced software development is in accordance with section 1.3.2, Sharing Institute Information or Information Assets with External Parties.

See also the Information Security Standard.

5.3.3 Control of Operational Software

Only Authorized Users may deploy software on operational systems.

5.3.4 Using Live Information for Testing

No one may use live Information for testing new vendor-supplied or custom systems or system changes unless the Information Owner has ensured that:

i. an analysis has been conducted of the foreseeable risks to BCIT arising from use and disclosure of live Information for system testing purposes;

ii. any identified risks have been suitably mitigated through appropriate Safeguards and that the same controls for the security of the Information as used in the production system are in place; and

iii. where applicable, the vendor has entered into a suitable contract with BCIT by which they are legally required to comply with all BCIT policies that apply to the Information.

5.3.5 Technical Vulnerability Management

The Cyber Security Officer and each IT Administrator must:

i. monitor information about the technical Vulnerabilities of BCIT Information systems;

ii. promptly evaluate the Institute's exposure to such Vulnerabilities; and

iii. take timely, appropriate measures to address the associated risks.

See the Information Security Standard.

6. Information Security Incident Management

6.1 Reporting Information Security Events and Weaknesses

6.1.1 Reporting Information Security Events and Weaknesses

Anyone who suspects an Information Security Incident has occurred or is likely to occur must report their suspicion to the Cyber Security Officer.

6.2 Management of Information Security Incidents and Improvements

6.2.1 Conduct of Investigations

a) The Cyber Security Officer must coordinate investigations into Information Security Incidents and must consult with the Privacy Office where Personal Information is likely to be involved.

b) While conducting an investigation, the Cyber Security Officer has authority to:

i. seize Information Assets;

ii. monitor access and use of Information Assets;

iii. record images; and

iv. make excerpts and copies of logs and backups.

6.2.2 Responsibilities and Procedures

All members of the BCIT community and all External Parties must provide timely assistance to an investigation when requested to do so by the Cyber Security Officer.

6.2.3 Investigation Limitations

The Cyber Security Officer may only investigate an individual's activities or files in response to an Information Security Incident or if the Cyber Security Officer has reasonable suspicion that the individual is engaging in activities that are noncompliant with BCIT policies.

6.2.4 Ensuring the Integrity of Information Security Incident Investigations

No one except the Cyber Security Officer may engage in investigational activities.

6.2.5 Learning from Information Security Incidents

The Cyber Security Officer must:

i. conduct reviews of major incidents after the incident; and

ii. periodically review incidents collectively to identify and understand trends that might be addressed to improve security efforts.

7. Business Continuity Management

7.1 Compliance with Business Continuity Policies

Business units must ensure that the Business Continuity of their Information and Information Assets complies with Policy 7110, Emergency Management.

7.2 Information Security Aspects of Business Continuity Management

7.2.1 Including Information Security in the Business Continuity Management Process

Business units must ensure that the planning and implementation of Business Continuity does not compromise Information Security.

7.2.2 Disaster Recovery Plan

System owners must:

i. ensure that Disaster Recovery plans for their systems are developed, tested, and implemented;

ii. negotiate appropriate recovery time with IT services or other service providers; and

iii. where business requirements exceed the ability to recover IT assets, establish mitigating controls.

8. Compliance

8.1 Compliance with Legal Requirements

8.1.1 Intellectual Property Rights (IPR)

All members of the BCIT Community and all External Parties must comply with Policy 6601, Intellectual Property.

8.1.2 Using Licensed Software

a) Business units must ensure that all software is appropriately licensed.

b) Authorized Users must comply with the terms and conditions of all End User License Agreements.

8.1.3 Protection of Organizational Records

All members of the BCIT Community and all External Parties must comply with Policy 6701, Records Management.

8.2 Information Systems Audit Considerations

a) Business units must ensure the planning and implementation of Information systems audits does not compromise Information Security.

b) Business units must ensure access to system auditing tools is protected against any misuse or compromise.

9. Non-Conforming Systems

Not all systems or technologies are capable of conforming in all details; when and

~~where applicable:~~

~~a) The Director of Enterprise Technology and the Cyber Security Officer must jointly maintain a list of systems and technologies that do not conform with this Policy 3502 and must ensure that the list:~~

~~i. includes a risk-based analysis focusing on non-conforming systems with the highest risk profile; and~~

~~ii. includes a reference to the risk assessment and risk management plan for each system or technology on the list.~~

~~b) System owners of systems that are unable to conform to this Policy 3502 and its Procedures must:~~

~~i. immediately report non-conformance to the Cyber Security Officer;~~

~~ii. undertake a risk assessment;~~

~~iii. develop a risk management plan; and~~

~~iv. submit the risk management plan to the Cyber Security Officer.~~

Consequences of Policy Violation

Compliance with this Policy is mandatory for all users of BCIT's IT Resources. Users in breach of this Policy or engaging in Misuse will be subject to discipline, up to and inclusive of dismissal or expulsion. BCIT reserves the right to restrict, suspend, or withdraw access to BCIT systems and services, including computing privileges and network connectivity.
Investigations of suspected Misuse and any resulting actions will follow established Institute procedures and principles of fairness and due process.

In cases where Misuse or other user equipment or activity poses an immediate security or operational risk, BCIT may take temporary measures to protect Institute systems, such as disconnecting or quarantining affected devices, until the issue is investigated and resolved.

Person Device connecting to BCIT networks may also be subject to reasonable security restrictions to protect Institute systems and data integrity.

Purpose

This policy establishes the Cyber Security Framework ensuring the security and reliability of BCIT's information technology resources ("BCIT technology assets" or "information assets"). It requires that all users, devices, and IT environments adhere to cybersecurity best practices, regulatory compliance, and risk management protocols to protect the confidentiality, integrity, and availability of BCIT information assets.

Roles and Responsibilities

Formatted: Font: 12 pt, Character scale: 100%

Formatted: Font: 12 pt, Not Bold, Character scale: 100%

Formatted: Heading 1, None, Indent: Left: 0 cm, Space Before: 0.1 pt, After: 0.1 pt, Line spacing: Multiple 1.08 li, Widow/Orphan control, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 3.53 cm

Formatted: Font:

Formatted: Font:

Formatted: Font:

Formatted: Font:

Formatted: Font:

Formatted: Indent: Left: 0 cm

Formatted: Font:

Roles	Duties and Responsibilities
BCIT Executive	The BCIT Executive is responsible for recommending an appropriate Information Security Framework to the Board of Governors, and for providing ongoing oversight of the Cyber Security Framework, including periodic independent reviews.
Chief Information Security Officer (CISO)	The CISO provides leadership and oversight for the security of BCIT's IT systems, data, and digital assets. Their responsibilities include developing and enforcing security policies, standards, ensuring compliance with applicable regulations and legislation, and maintaining a secure infrastructure capable of detecting, preventing, and responding to cyber threats. The CISO is the final authority for approving security exceptions.
Chief Financial Officer (CFO)	The CFO is responsible for reviewing requests to implement or operate electronic commerce systems or systems that store or process personal payment information, approving or denying such requests, and establishing any conditions that must be met.
Chief Information Officer (CIO)	The CIO provides strategic leadership and oversight for all aspects of enterprise technology at the Institute. This role encompasses shaping the overall technology strategy and fostering innovation to meet the evolving needs of BCIT community. The CIO is responsible for selecting, configuring, and supporting IT-issued devices, as well as providing communication tools such as email, messaging services, VOIP telephony, and audio/video conferencing.
Department Head / Dean (Business Owner)	Also referred to as Business owner. They are responsible for the oversight and governance of data within their academic or administrative unit. They act as the primary authority on how data should be classified, accessed, used, and protected, ensuring alignment with Institute cybersecurity policies and applicable laws such as the *Freedom of Information and Protection of Privacy Act* ("FIPPA" or the "Act") .
IT Administrators	Are responsible for the technical management and system configuration and implementation of required controls as per policy and standards (System Administrators, Database Administrators, Network Administrators, etc.).
IT Asset Owner	A designated individual or role responsible for ensuring that an IT asset is classified, properly used, protected, and maintained in accordance with BCIT's information security policies, standards, and procedures. This includes both physical and digital assets such as computers, servers, software, data, and network devices.
Director, Privacy, Information Access and Policy Management	The person responsible for overseeing and administering the process for completing and documenting Privacy Impact Assessments (PIAs) for all new systems, projects or programs, as required under the *Freedom of Information and Protection of Privacy Act* (FIPPA). A PIA is a risk management and compliance tool used to identify and address

	potential privacy and security risks. The Information Access and Privacy Office provides ongoing support to all Users to ensure that BCIT's use of Information Technology aligns with privacy protection requirements under FIPPA.
Director, Enterprise Risk & Internal Audit	The person responsible for identifying and assessing Institute risks, including those relating to the Cyber Security Framework.
End Users	Users must adhere to cybersecurity policy and report incidents promptly.
Third Parties	Contractors, vendors, and other external parties must comply with contractual and policy-related security requirements.

BCIT Commitment to Cyber Security Risk Management

BCIT is committed to a proactive and risk-informed approach to cybersecurity. This includes identifying, assessing, managing, and mitigating cybersecurity risks in alignment with institute objectives, regulatory requirements, and best practices. We strive to cultivate a culture of security awareness and shared responsibility across all levels of the organization. To uphold this commitment, BCIT will:

a) Establish and maintain a comprehensive cybersecurity risk management framework.
b) Continuously evaluate and strengthen controls that protect Institute digital infrastructure and sensitive information.
c) Regularly monitor the evolving threat landscape and adjust risk mitigation strategies accordingly.
d) Ensure cybersecurity roles, responsibilities, and accountability are clearly defined and understood across the Institute.
e) Promote collaboration between IT, academic, and administrative units to ensure security is embedded in all processes and technologies.
f) Provide ongoing education, training, and resources to support cybersecurity awareness and readiness.
g) Conduct regular assessments and report cybersecurity risks, incidents, and mitigation progress to senior leadership and governance bodies.

By embedding cybersecurity risk management into BCIT's strategic and operational planning, we aim to safeguard our digital environment and support innovation, learning, and Institute resilience.

Cyber Security Framework Domains

1. **Cyber Security Governance**

   The CISO is responsible for overseeing the implementation of cybersecurity policies and standards, including compliance and enforcement. Due to the dynamic nature of cyber threats, evolving regulatory landscapes, and our strategic objectives, policies and standards are not static. They are regularly reviewed and updated to maintain relevance, effectiveness, and adaptability.

Formatted: Indent: Left: 1.27 cm

A key element of the governance framework is the establishment of specialized Security Working groups. Among them, the SecOps ("Security Operations") Working Group plays a critical role in developing security standards. These standards then advance to the Cybersecurity Standards Committee for comprehensive review and endorsement, followed by final approval by the CISO. This multi-tiered approach ensures security standards are thoroughly vetted and refined before adoption.

2. Risk Management

BCIT is committed to proactively identifying, assessing, and managing cybersecurity risks by embedding risk management into decision-making processes, project lifecycles, and technology operations. All risks must be documented, evaluated, and addressed through mitigation, transfer, acceptance, or avoidance, in accordance with BCIT's risk appetite, risk tolerance, and compliance obligations. Risk assessments must be conducted regularly and in response to significant changes in systems, services, and emerging threats.

In compliance with FIPPA, a Privacy Impact Assessment (PIA) must be completed for all new initiatives. When sensitive personal information is disclosed or stored outside Canada, a Security Threat Risk Assessment (STRA) must also be conducted in collaboration with the Information Access and Privacy Office (IAPO). These assessments ensure that technical, legal, and operational risks are fully identified and appropriately mitigated. For detailed guidance, refer to the ***Cyber Security Risk Management Standard***.

3. Identity & Access Management (IAM)

BCIT must implement robust Identity and Access Management (IAM) practices to ensure that access to information systems and data is granted based on the principles of least privilege, role-based access, and need-to-know. All user identities must be uniquely identifiable and authenticated before access is permitted. Access rights be regularly reviewed, promptly updated upon role changes or departures, and revoked when no longer required. All remote access to BCIT systems must be secured, authorized, and monitored to ensure the protection of Institute data and services. Multi-factor authentication (MFA) must be employed for systems containing BCIT sensitive or Personal Information. Systems that cannot meet current access requirements due to technical constraints should be treated as exceptions (see Policy Section 23). For detailed guidance, refer to the ***Identity and Access Management and Access Control Standard.***

4. IT Asset Management

BCIT must employ a systematic process for managing and tracking all IT assets to ensure that they are properly protected, maintained, and securely disposed of. Proper IT asset management allows the Institute to maintain control over its technological infrastructure, minimize security vulnerabilities, optimize asset utilization, and comply with applicable laws and regulations.

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

The IT Asset Management program will ensure that all information technology assets, hardware, software, and virtual/cloud resources, are accurately assigned owners, and are inventoried, tracked, and managed throughout their lifecycle.

4.1 System Categorization

Business Owners must classify all information systems based on sensitivity, business criticality, and potential impact. This classification will guide the application of security controls, risk management, and compliance measures. Critical or sensitive systems will have enhanced monitoring, incident response, and recovery protocols. In a security incident, system classification will determine response urgency, choice of procedures, and escalation to ensure effective mitigation, recovery, and communication. For a detailed guide, refer to the ***System Categorization and IT Asset Management Standard.***

5. Data Protection and Privacy

BCIT is dedicated to safeguarding the confidentiality, integrity, and availability of its information assets while upholding the privacy rights of individuals whose data it collects, processes, and stores. As a public institution, BCIT complies with FIPPA, governing the collection, use, disclosure, and protection of personal information. The institute ensures transparency and accountability in its operations and is committed to protecting the privacy of its staff, students, and the broader community.

To support this commitment, all Institute data must be classified based on its sensitivity, criticality, and applicable regulatory requirements. Information is categorized according to its potential impact on BCIT, its community, and external stakeholders if disclosed, altered, or lost. This classification framework enables risk-based decision-making, supports compliance with legal and regulatory obligations (such as FIPPA,, and PCI-DSS), and facilitates secure information sharing across academic, research, and administrative functions. All faculty, staff, students, contractors, and third-party service providers are responsible for handling data appropriately, and ensuring safeguards are in place to prevent unauthorized access, use, disclosure, or destruction.

5.1 Information and Data Classification

BCIT implements a risk-based approach to information and data protection through formalized information and data classification, access control, retention, and secure disposal practices. Data should be securely managed throughout its lifecycle, including collection, storage, processing, transmission, and destruction.

Business Owners are accountable for classifying, protecting, and ensuring appropriate access to the data under their stewardship in accordance with BCIT cybersecurity and data governance policies. They must work with ITS and CSO teams to: apply appropriate safeguards based on the sensitivity and criticality of the data, manage data sharing, and respond to data-related risks or incidents. The following table outlines BCIT's information security classification:

Information Classification Levels	Description	Examples

Formatted: Font:

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Tab stops: 2 cm, Left + Not at 1.27 cm

PUBLIC INFORMATION		
PUBLIC - Applies to data and Information, that if compromised, would not result in injury to individual, or to BCIT or its partners	Information that is readily available to the public	• BCIT website • Brochures • Course descriptions • Published marketing information • Job postings
PROTECTED INFORMATION	Information that is restricted by a designated level of security and access control	
PROTECTED A – Applies to data and information that if compromised, could cause injury to an individual, or harm to BCIT and partners.	Information requiring a reasonable level of security controls with varying degrees of access control	• Administration procedures • Vendor or service provider • Departmental policies and procedures • Teaching materials
PROTECTED B – Applies to data and information that, if compromised, could cause serious injury to an individual, or serious harm to BCIT and its partners.	Information requiring the highest levels of security controls with varying degrees of access controls	• Research data and intellectual property • Drafts of strategic plans • Penetration testing reports • Locations of hazardous material storage
PROTECTED C – Applies to data and information that, if compromised, could cause grave injury to an individual or severe harm to BCIT and its partners	Information requiring the highest level of security controls with the highest degree of access control	• Social Insurance Numbers • Medical information • Financial information • Passwords and passphrases

5.2 Data Retention and Disposal

All BCIT data must be retained in accordance with applicable legal and regulatory obligations, and in compliance with BCIT Policy 6701-Records Management. Unauthorized deletion, alteration, or inappropriate storage of institutional data is prohibited. And data that is no longer required must be securely disposed of through approved data destruction methods as per the ***Secure Media Destruction Standard.***

5.3 Secure Transmission and Sharing of BCIT Electronic Data

BCIT will implement measures to ensure secure transmission and sharing of electronic information. All data, especially confidential information, must be transmitted using secure methods, including encryption and authenticated access, to prevent unauthorized access. Internal and external data sharing should occur through approved secure channels, and users must follow BCIT protocols. Data sharing is restricted to a need-to-know basis with documented authorization.

BCIT prohibits using insecure methods, such as unencrypted email or unauthorized file-sharing platforms, for sensitive data transmission. Users must adhere to secure communication practices, including strong authentication, encryption, and vigilance against phishing, malware, and social engineering. Unauthorized use, disclosure, or interception are prohibited and subject to disciplinary action. Refer to the ***Secure Transmission and Sharing of BCIT Electronic Information Standard.***

5.4 Payment Card Data Security

BCIT must comply with all applicable PCI DSS standards based on its merchant level.

To ensure compliance, the following controls must be implemented:

i. **System Approval** - Payment systems must be approved by the Chief Financial Officer before implementation.
ii. **Data Encryption** - Cardholder data must be encrypted during both transmission and storage.
iii. **Access Control** - Only authorized personnel may access payment systems, and all access must be monitored.
iv. **Fraud Prevention** - Systems must include safeguards to prevent fraud, unauthorized disclosure, and data manipulation.
v. **Third-Party Agreements** - External service providers that process payment card transactions or integrate with BCIT systems handling cardholder data must enter into binding agreements requiring full compliance with BCIT's cybersecurity policies and applicable PCI DSS requirements.
vi. **Secure System Design** - Systems must be designed to ensure confidentiality, integrity, and availability of payment information.
vii. **Vulnerability Scanning Compliance** - The Institute shall conduct regular internal and external vulnerability scans on systems that store, process, or transmit cardholder data, in accordance with PCI DSS requirements. These scans must be performed by qualified personnel or approved scanning vendors and documented for compliance validation.

6. Encryption

BCIT must employ the most current encryption mechanisms to protect sensitive data both in transit and at rest across all systems, networks, and devices, including removable media. Encryption must be implemented using current or higher industry-standard protocols and algorithms to prevent unauthorized disclosure, alteration, or destruction of Institute data. For more detailed guidance refer to the ***Encryption Requirement and Cryptographic Controls Standards***.

7. Network Security

To safeguard BCIT's IT and operational technology (OT) environments, comprehensive network security controls must be implemented. This includes enforcing strong access controls to defend against Advanced Persistent Threats (APTs), continuously monitoring all network segments for unauthorized access, anomalies, and potential cyber threats, and conducting security assessments or penetration testing following any significant network changes to identify and mitigate associated risks. For a detailed guide refer to the ***Network Security and Segmentation Standard.***

7.1 IP Address Assignment and Management

BCIT must maintain a centralized and secure system for managing all assigned Internet Protocol addresses (both IPv4 and IPv6) to ensure proper allocation, accountability, and protection of networked resources. All IP address assignments must be authorized and documented by the central IT department or designated authority. Unauthorized use or reallocation of IP addresses is prohibited. IP address management must support network segmentation, access control, incident

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

response, and compliance with security monitoring and auditing requirements. For a detailed guide refer to the ***IP Address Management Standard.***

7.2 Domain Name Management

BCIT must maintain centralized oversight and control of all Institute domain names to ensure integrity, security, and alignment with official branding and communication standards. Registration, renewal, configuration, and Domain Name System management must be conducted by authorized personnel following established security practices, including secure registrar accounts, Domain Name System Security Extensions (where applicable), and change control procedures. Unauthorized registration or use of BCIT-affiliated domains is strictly prohibited. For a detailed guide refer to the ***Network Security and Segmentation Standard.***

8. Endpoint Security

BCIT must implement and enforce comprehensive endpoint security controls on all devices that access the institute information systems. This includes the use of standardized configurations, malware protection, device encryption, access control, and continuous monitoring to safeguard endpoints against evolving cyber threats. For a detailed guidance reference the ***System Security Hardening Standard*** and ***Vulnerability, and Patch Management Standard.***

9. Third-Party and Supply Chain Risk Management

BCIT must establish a structured Third-Party and Supply Chain Risk Management program to identify, assess, and manage cybersecurity risks associated with external entities. All third-party engagements must undergo thorough due diligence, incorporate defined security requirements within contracts, and be subject to continuous risk monitoring to safeguard Institute assets from unauthorized access, improper use, and operational disruptions.

BCIT may, on a case-by-case basis, host data or systems on behalf of third-party organizations, including affiliated non-profit entities. Where such arrangements exist, they should follow and adhere to the requirements outlined in the ***Third Party and Supply Chain Security Standard***.

10. User Awareness and Training

BCIT must establish and maintain an ongoing cybersecurity awareness and training program to ensure that all users (staff and students, contractors, and third-party vendors) understand their responsibilities in protecting BCIT's information and technology assets. All BCIT users should complete cybersecurity awareness training as part of onboarding and participate in refresher training at least annually or as needed based on emerging threats or regulatory changes. The Cybersecurity Office will periodically conduct phishing simulations to evaluate awareness.

11. Physical and Environmental Security

Formatted: Font: (Default) +Body (Calibri)
Formatted: Font: (Default) +Body (Calibri), Font color: Auto
Formatted: Font:
Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left
Formatted: Font:
Formatted: Font: (Default) +Body (Calibri), Font color: Auto
Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left
Formatted: Font:
Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left
Formatted: Font:
Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

BCIT must implement and maintain comprehensive physical and environmental security controls to protect all sensitive areas, equipment, and assets from unauthorized access, damage, and disruption. These controls encompass both physical access limitations and environmental protections, helping to ensure protection of BCIT systems. Access to critical areas, including data centers, research and student labs, and administrative buildings, must be restricted to authorized personnel only. For more detailed guidance refer to the ***Data Center Physical Security Standard***.

12. Application Security

BCIT is committed to securing all applications throughout their lifecycle, including those developed internally, externally acquired, or created through industry-sponsored student projects. All applications must adhere to secure development practices to safeguard Institute data from unauthorized access, tampering, and service disruptions. No application may be deployed to production without a security review and CISO approval.

All application environments including, development, testing, staging, and production must be clearly segregated to prevent unauthorized access and cross-environment impact. Access must follow the principle of least privilege, granting users only the minimum necessary permissions based on their approved roles. All application security practices must align with recognized industry standards and frameworks to ensure consistent risk management across BCIT's digital ecosystem. For a detailed guide on Application Security, refer to the ***Secure Application Development and Modification Standard.***

13. Database Security

BCIT must enforce strong security controls across all Institute databases, relational and non-relational, to prevent unauthorized access, data tampering, and unplanned disruptions; ensuring data remains secure, accurate, and reliably accessible. All databases must adhere to recognized cybersecurity frameworks such as National Institute of Standards and Technology and Center for Internet Security, including access controls, encryption, vulnerability assessments, and audit logging.
Database administrators must enforce role-based access, restricted to authorized personnel and fully auditable. Databases containing sensitive or critical data require enhanced safeguards and regular security reviews. Security measures must be applied consistently throughout the database lifecycle, from design to deployment and ongoing management. For more detailed guidance refer to the ***Database Management Security Standard***.

14. Vulnerability and Patch Management

BCIT must implement and maintain a proactive vulnerability and patch management program across all IT, OT, and IoT environments to mitigate risks from known software and firmware weaknesses. Systems and applications must be regularly assessed, with vulnerabilities remediated based on risk severity and criticality.

Security patches must be applied promptly and in a controlled manner, following industry best practices and approved cybersecurity standards. Business units responsible for asset management must ensure periodic vulnerability scans and maintain auditable records of remediation or mitigation actions. Special attention must be given to systems handling

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

sensitive BCIT data. For more detailed guidance, refer to the ***Vulnerability and Patch Management Standard.***

15. Change Management

BCIT must implement a formal change management process to ensure all changes to hardware, software, configurations, or procedures are reviewed, tested, approved, and documented to minimize risks to security, performance, and availability. All changes must be assessed for security impact prior to implementation. Changes must be authorized by the Change Advisory Board or designated approvers. Emergency changes must follow an expedited approval process and undergo a post-implementation review. Post-implementation monitoring is required to verify expected outcomes and ensure no adverse effects on security or performance.

16. Business Continuity Management

BCIT is committed to implementing and maintaining a Business Continuity Management program that ensures resilience against cyber threats and operational disruptions. All critical business functions and information systems must have documented, tested, and regularly updated continuity and recovery plans that align with BCIT 's risk tolerance and regulatory requirements. For more detailed guidance see also **Policy 7110, Emergency Management.**

17. Backup & Disaster Recovery

BCIT must implement effective backup and disaster recovery practices to safeguard critical data and IT infrastructure. Regular, secure backups and well-defined disaster recovery processes are essential to minimize operational downtime, prevent data loss, and maintain business continuity in the event of a disaster or cyber incident.

***17.1 Redundancy* & Infrastructure Resilience**

BCIT must design, implement, and maintain redundant and resilient infrastructure to minimize service disruptions from hardware failure, cyber-attacks, or natural disasters. Infrastructure supporting mission-critical services must also include failover capabilities, and geographic distribution to ensure continuity and integrity. For more detailed guidance refer to the ***Backup and Recovery Management Standard.***

18. Incident Response & Monitoring

BCIT must maintain a formal Incident Response program to promptly identify, contain, investigate, and remediate cybersecurity incidents. All employees, contractors, and third-party partners must report suspected incidents immediately. Designated IR teams will follow documented procedures to minimize impact and prevent recurrence. Dedicated Incident Response Plans must be in place for both IT and OT environments. Regular cybersecurity tabletop exercises must be conducted to test response readiness and assess system resilience.

18.1 Incident Response & Activation

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Line spacing: single, Tab stops: 2 cm, Left

In the event of an incident (cyber related or disaster), the Cyber Security Incident Response Team (CSIRT) immediately assesses the situation and activates the appropriate IT Recovery Plan. A structured Incident Response Framework be used to contain, mitigate, and recover cyber threats or system failures. The CISO must test and maintain a detailed ***Cyber Security Incident Response Plan.***

18.2 Emergency Authority

If an emergency arises that threatens the security of Institute systems or data, the CISO has the authority and responsibility to implement emergency response measures to shut down the risk and to mitigate further damage. Those affected by such actions must be notified as soon as practicable. The CISO will immediately report any such emergency response measures to the BCIT Executive, and both will work to evaluate the risk and review next steps.

19. Cloud Security

BCIT must ensure the secure adoption and use of cloud services in alignment with its cybersecurity policies, standards, and applicable legal and regulatory obligations, including FIPPA. All cloud-based systems and data must follow principles of data classification, access control, encryption, and vendor risk management to safeguard Institute information and maintain accountability under a shared responsibility model.

Before implementation, cloud services must be assessed and approved by an appropriate BCIT governance committee or equivalent authority. Any service involving the collection, use, or disclosure of personal information requires a Privacy Impact Assessment (PIA) in accordance with FIPPA. If personal information is stored or processed outside of Canada, a Security Risk Assessment must also be conducted in collaboration with the Information Access and Privacy Office (IAPO) to identify and mitigate legal, technical, and operational risks. For more detailed guidance, reference the ***Cloud Security and Compliance Standard.***

20. Human Resources Security

Human Resource Security is critical to the protection of Institute information and IT systems. BCIT must ensure that all staff, contractors, and third-party vendors understand and fulfill their cybersecurity responsibilities. This includes ensuring proper screening, training, access control, and monitoring throughout the employee's life cycle.
Human Resource Security practices aim to minimize the risk of human errors, insider threats, or breaches resulting from personnel mishandling BCIT sensitive data or systems.

21. Email Security & Privacy

i. All electronic communications on BCIT systems must be safeguarded against unauthorized access, use, disclosure, or disposal through reasonable security measures.
ii. Users must transmit messages, attachments, and shared information securely using approved platforms. Sensitive or regulated data requires encryption and other protective controls.
iii. BCIT communication systems are subject to monitoring and auditing under Institute policies, applicable laws, and cybersecurity best practices. While privacy protections

Formatted: Font:
Formatted: Indent: Left: 1.27 cm, Tab stops: 2 cm, Left
Formatted: Font:
Formatted: Indent: Left: 1.27 cm, Tab stops: 2 cm, Left
Formatted: Font: (Asian) Japanese
Formatted: Font: (Default) +Body (Calibri), Font color: Auto
Formatted: Font:
Formatted: Indent: Left: 1.27 cm, Tab stops: 2 cm, Left

exist, communications may be accessed to ensure compliance and protect Institute integrity.

iv. Access to user email or electronic communications will occur only under authorized, lawful circumstances (e.g., investigations, operational continuity, legal obligations) with prior approval from designated authorities. Confidentiality and due process will be maintained.

v. Unauthorized use of personal email accounts for BCIT business is prohibited. Automatic forwarding of BCIT email (@bcit.ca) to non-BCIT accounts is not permitted. Refer to the **Secure Transmission and Sharing of BCIT Electronic Information Standard** for detailed guidance.

22. Compliance and Monitoring

BCIT must implement continuous compliance and monitoring practices to ensure adherence to institute cybersecurity policies, technical standards, regulatory requirements, applicable laws and industry approved standards. Systems, networks, and user activities may be monitored and audited regularly to detect violations, assess risk, and enforce security controls. All monitoring respects privacy laws and ethical guidelines while ensuring the integrity and security of BCIT information systems. For more detailed information refer to the ***Logging and Monitoring Standard.***

23. Exceptions

In exceptional circumstances where full compliance with cybersecurity policies is not feasible, a formal exception may be requested. All security policy exceptions must be documented, assessed for risk, and approved through BCIT's Cybersecurity Risk Management process, with final authorization by the CISO or their delegate. Approved exceptions must include compensating controls to mitigate associated risks and will be subject to periodic review, at least biannually or upon any significant system or operational changes.

APPENDICES

A. Technical Standards Associated with This Policy

Information Security Standards - https://authc.bcit.ca/it-services/secure/

~~a) BCIT may terminate or restrict the access privileges of a user whose activities negatively affect or pose a Threat to a facility, another account holder, normal operations, or the reputation of the Institute.~~

~~b) Following due process, the Institute may take one or more of the following actions against any user whose activities are in violation of this Policy 3502 or the applicable law:~~

~~i. a verbal or written warning;~~

~~ii. restrictions on access or removal of access to any or all Institute computing facilities and services;~~

~~iii. legal action that could result in criminal or civil~~

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Tab stops: 2 cm, Left

Formatted: Font:

Formatted: Indent: Left: 1.27 cm, Tab stops: 2 cm, Left

Formatted: Indent: Left: 1.27 cm, Hanging: 0.63 cm

~~proceedings;~~

~~iv. in the case of students, disciplinary action under Policy 5102, Student Code of conduct (Non-Academic); and~~

~~v. in the case of employees, disciplinary action up to and including termination.~~

~~c) BCIT may immediately disconnect, quarantine, or otherwise contain equipment, and may seize Institute-owned equipment, that violates BCIT policy or negatively affects or poses a Threat to a facility, normal operations, or the reputation of the Institute.~~

~~Procedures Associated With This Policy~~

~~1. Procedure 3502-PR1, Information Security Procedures~~

~~Forms Associated With This Policy~~

~~None.~~

B. Amendment History

			Approval Date	Status
1.	Creation:	Policy 3502 version 1	2009 Jan 27	Replaced
2.	Revision:	Policy 3502 version 2	2016 Oct 04	Replaced
3.	Revision:	Policy 3502 version 3	2020 May 26	In Force
4.	Revision: Policy 3502 (draft) version 4		yyyy mm dd	Pending

C. Scheduled Review ~~Date~~ and Updates

This policy must be reviewed no later than five years from approval (next review date 2030 Dec 02 pending approval). However, it may be updated as needed to address emerging threats and changes in technology or regulatory requirements.

D. Definitions

Term	Definition
Asset Custodian	BCIT employee who has been assigned custody and control of an Information Asset.
Authentication	A process of verifying the identity of a user, system, or device before granting access to resources, applications, or services.
Authorization	The granting of permission in accordance with approved policies and procedures to perform a specified action on an Information Asset.
Business /Academic Head	The Dean, Director, or other person who has been assigned responsibility for a business unit.
Business Continuity	The Institute's ability to maintain or restore its business and academic services when some circumstance threatens or disrupts normal operations. (See Policy 7110, Emergency Management).

Formatted: Font: 12 pt, English (United States), Kern at 16 pt

Formatted: Font: 12 pt, English (United States)

Formatted: Heading 2, Space Before: 0.1 pt, After: 0.1 pt, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 1.27 cm + Indent at: 1.9 cm

Formatted: Font: 12 pt, English (United States), Kern at 16 pt

Formatted: Font: 12 pt, English (United States)

Formatted: Heading 2, Space Before: 0.1 pt, After: 0.1 pt, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 1.27 cm + Indent at: 1.9 cm

Formatted: Font: Font color: Auto, Kern at 16 pt

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 1.27 cm + Indent at: 1.9 cm

Business Owner	The BCIT employee who has been assigned responsibility for overseeing the lifecycle of one or more types of Information including responsibility for classifying and protecting Information.
BYOD	Refers to "bring your own device" and means a Mobile Device or Removable Media that is owned by the user.
Chief Information Officer (CIO)	BCIT Chief Information Officer.
Chief Information Security Officer (CISO)	BCIT Chief Information Security Officer.
Confidential Information	Any data or information that is meant to be kept private and secure, and whose unauthorized access, disclosure, or exposure could harm individuals or BCIT.
Contact Information	Means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone numbers, business address, business email or business fax number of the individual.
Contractors	An individual or entity engaged under contract to perform specific work or services for BCIT, and who may require access to BCIT systems, facilities, or information assets during the course of their engagement.
CSO	Cyber Security Office.
Data	Data refers to raw, unprocessed facts, figures, or symbols that are collected, generated, or received by BCIT systems, individuals, or processes. Data may exist in digital, physical, or verbal form and becomes information when it is organized, interpreted, or contextualized to convey meaning.
Disaster Recovery	The activities that restore the Institute to an acceptable condition after suffering a disaster. See Policy 7110, Emergency Management for more information.
Encryption	The process of converting information or data into a coded format to make it unreadable, to prevent unauthorized access.
End Users	Individuals who interact with the system, application, or service on a daily basis. They are the final point of interaction in the technology chain and are usually not involved in the development or maintenance of the system.
ERM	BCIT Enterprise Risk Management
FIPPA	*Freedom of Information and Protection of Privacy Act* (BC)
Firewall	A system designed to prevent unauthorized access to or from a private network or between network zones.
GDPR	General Data Protection Regulation.
Information	Refers to all forms of institutional knowledge, data, and record, whether digital, physical, or verbal, that are created, stored, transmitted, or processed by BCIT. Information is considered an asset and must be protected against unauthorized access, disclosure, alteration, or destruction to preserve its confidentiality, integrity, and availability.

Information Security	The preservation of confidentiality, integrity, and availability of information. Confidentiality ensures that information is accessible only to authorized users. Integrity involves safeguarding the accuracy and completeness of information and processing methods. It may also include authenticity, auditability, accountability, non-repudiation, and reliability of information. Availability ensures that Authorized Users have access to IT assets when required.
Information Security Classifications	The information security categories are described in section 5.1 *Information Security Classifications.*
Information Technology (IT) Asset	Any device, system, software, application, data, or network component that is owned, leased, or managed by BCIT, or otherwise used to store, process, transmit, or secure institutional information. IT Assets include computing devices, servers, mobile equipment, cloud and network services, and digital information repositories that support BCIT's teaching, learning, research, and administrative operations.
IOT	Internet of Things
ITS	BCIT Information Technology Services.
Mobile Device	Includes any electronic device that is portable and contains Information, or has the ability to contain Information, or provides the ability to access or transmit Personal Information or Protected Information. Examples include laptops, tablet PCs, and any smart mobile devices.
OT	Operational Technology
PCI-DSS	Payment Card Industry Data Security Standard
Personal information	Means recorded information about an Identifiable Individual other than contact information
Removable Media	Information storage devices that are not fixed inside a computer. Examples include external hard drives, CD-ROMs, DVDs and USB flash drives.
Safeguard	A method of managing risk, including policies, procedures, practices, or BCIT structures, which can be of a physical, administrative, technical, management, or legal nature.
SCADA	Supervisory Control and Data Acquisition
Third-party service provider	An external organization engaged to deliver services on behalf of BCIT, which may involve access to, processing of, or storage of BCIT's data, systems, or networks.
Threat	Any potential event, action, or actor that could exploit a vulnerability to cause harm to a system, network, or BCIT.
Vendor	An external entity that supplies goods, technology, or software to BCIT, either through purchase, license, or subscription, and may have access to BCIT IT assets depending on the nature of the product or service and contract.
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more Threats.

E. Related Documents and Legislation

Formatted: Font: Font color: Auto, Kern at 16 pt

Formatted: Font: Font color: Auto, English (United States), Kern at 16 pt

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 1.27 cm + Indent at: 1.9 cm

Law/Regulation/Policy	Document Name
BC legislation	*College and Institute Act*, RSBC 1996, c 52 *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 *Personal Information Protection Act*, SBC 2003, c 63
Federal legislation	*Criminal Code*, RSC 1985, c C-46 *Copyright Act*, RSC 1985, c C-42 Canada's Anti-Spam Legislation (i.e. CASL)[1]
Industry Standards	PCIDSS, Payment Card Industry Security Standards published by the Payment Card Industry Security Standards Council, including the "PCI Data Security Standard", the "PIN Transaction Security Requirements", and the "Payment Application Data Security Standard" NIST 800-82, (Guide to Industrial Control Systems Security) IEC 62443, (Industrial Automation and Control System Security) NERC CIP, (Critical Infrastructure Protection for energy systems) ISO 27001, (Information Security Management Systems) CIS Controls (Control 07: Continuous Vulnerability Management) NIST SP 800-40 Rev. 3, NIST SP 800-53, NIST SP 800-37 Rev. 2 CIS Controls v8 (Control 16: Application Software Security) NIST SP 800-218 (Secure Software Development Framework - SSDF) OWASP Top 10
BCIT Policies	1500, Code of Conduct 3501, Acceptable Use of Information Technology 5102, Student Code of Conduct (Non-Academic) 5900, Education Technology 6601, Intellectual Property 6700, Freedom of Information and Protection of Privacy 6701, Records Management 7506, Use of Materials Protected by Copyright 7170, Protection of Equipment and Property 7110, Emergency Management

~~2025 May 26~~

DECISION NOTE
November 20, 2025

PREPARED FOR: Board of Governors

PREPARED BY: Shawna Waberi, Chair, Education Council

ISSUE: Admissions and Recognition of Prior Learning – Procedure #5003-PR1

APPENDICES:

1. Appendix A: Admissions and Recognition of Prior Learning - Procedure #5003-PR1, draft
2. Appendix B: Admissions and Recognition of Prior Learning - Procedure #5003-PR1, redline

RECOMMENDATION:

THAT the Board of Governors approves the revised *Admissions and Recognition of Prior Learning Procedure - #5003-PR1*.

BACKGROUND:

On November 18, 2025, the Governance Committee reviewed and recommended the revised procedure for Board approval. The Education Council then endorsed presenting the procedure at their meeting on November 19.

Admissions and Recognition of Prior Learning Policy and Procedure were updated in February 2024. This revision is to align to language in *Program Suspension and Cancellation - Policy #5405* that speaks to cancellation and suspension.

SUMMARY:

Following a request from the Registrar and discussions with the Policy Management Office a minor update in wording of the procedure was made to provide clarity to address situations in which BCIT must revoke an offer of admission due to program suspension or intake cancellation. This change is deemed “non-substantive” for the purpose of bypassing the 30-day community review, by executive sponsor, Jennifer Figner, Provost and VP Academic.

The following revisions were made (new text in bold):

PR-1 Appendices A and B:

- The program is cancelled **or suspended** prior to the start of classes.
- **A program intake is cancelled, and admission cannot be deferred to a future offering.**

ADMISSIONS AND RECOGNITION OF PRIOR LEARNING – PROCEDURE #5003-PR1

REVISED DRAFT

BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

Admissions and Recognition of Prior Learning [draft amendment]

Procedure No:	5003-PR1
Version:	6
Policy Reference:	5003 – Admissions and Recognition of Prior Learning
Category:	Education
Approval Body:	Board of Governors (on advice of Education Council)
Executive Sponsor:	Provost and VP Academic
Department Responsible:	Registrar's Office
Directory of Records Class:	0650-10
Approval Date:	[yyyy mmm dd] *tbd*

Objectives

This Procedure describes processes and criteria for admission consideration, application assessment, and recognition of prior learning at BCIT.

Table of Contents

Who This Procedure Applies To

This procedure applies to:

- Applicants who are seeking admission consideration into BCIT and/or a specific BCIT program.

- Applicants or students who are seeking recognition of prior learning.
- The Registrar, Deans, Directors, Instructors, and other BCIT employees responsible for evaluating student applications or assessing prior learning.

Related Documents and Legislation

Federal

Constitution Act, 1982
Immigration and Refugee Protection Act, SC 2001, c 27
Canadian Association for Prior Learning Assessment: Quality Assurance for the Recognition of Prior Learning in Canada, 2015
Truth and Reconciliation Commission of Canada: Calls to Action, 2015

Provincial

College and Institute Act, RSBC 1996, c 52
Criminal Records Review Act, RSBC 1996, c 86
Declaration on the Rights of Indigenous Peoples Act, SBC 2019
Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165
Human Rights Code, RSBC 1996, c 210
BC Council on Admissions and Transfer [BCCAT]: Policies 1A, 3A, 3B.2, Principles and Guidelines for Transfer

BCIT

Policy 2300, Fees and Charges
Policy 2502, Signing Authority
Policy 5102, Student Code of Conduct (Non-Academic)
Policy 5104, Student Code of Academic Integrity
Policy 5402, Program Review
Policy 5405, Program Suspension and Cancellation

Definitions

Definitions are incorporated within the policy and procedure.

Duties and Responsibilities

Included in this Procedure.

Admissions Procedure

1 Application Submission and Deadlines

a) Applicants apply or declare to BCIT through EducationPlannerBC or BCIT's Website. Applicants may apply for more than one program.
b) Applicants for apprenticeship programs submit an Apprentice Training Request and do not follow the standard admissions assessment process.
c) An application will be complete when all required documentation and the application fee have been received.

d) Official or certified documentation supporting an application must be received by BCIT to consider an offer of admission. BCIT only considers English language documents or certified English translations of documents in the admissions process except for documents from francophone schools in Canada. Academic transcripts completed outside of Canada may require a comprehensive or basic international credential evaluation by a member of the Alliance of Credential Evaluation Services of Canada. All application documents become the property of BCIT and will not be returned.

e) Application deadlines for competitive admission programs are listed on BCIT's website. Late applications may be considered on an individual basis subject to seat availability. Applications that do not comply with all posted deadlines will be cancelled.

2 Application Review

a) The Admissions Office ("Admissions") will:
   i. Assess the applicable academic admission requirements for completed applications;
   ii. Provide programs with proposed application processing dates for program assessments;
   iii. Be responsible for posting and updating equivalencies for academic admissions requirements.

b) Program areas will:
   i. Assess the applicable non-academic admission requirements for completed applications.

c) Applicants satisfying the minimum admission requirements will be considered qualified applicants eligible for admission evaluation.

d) Assessment of program choices if applicants apply for more than one program:
   i. First-choice program applications will be assessed first. If an applicant is eligible for admission, the applicant's second-choice program application will not be assessed.
   ii. Second-choice programs will be assessed if the applicant is not admissible to their first-choice program. Admissions reserves the right to assess second-choice program applications even if the applicant is admissible to their first-choice program.

3 Applicant Types

a) General Applicants may have academic history from the following categories:
   i. Canadian provincial secondary school curriculum: BCIT academic admission requirements are based on the British Columbia Certificate of Graduation or Adult Graduation Diploma curriculum. Applicants following other Canadian provincial secondary school curricula will be required to present provincial equivalencies. Applicants who have completed home-schooling will be considered on an individual basis and may require supplementary evidence of academic ability. The Registrar's Office is responsible for posting and updating provincial equivalents.

ii. Non-Canadian secondary school curriculum: Applicants must present secondary school graduation from an approved and recognized institution within an education system that comprises 12 years of primary and secondary study or equivalent. Satisfactory completion of non-Canadian secondary school may not be, on its own, an acceptable basis for admission. In such cases, applicants may be considered with alternate assessment criteria.

iii. Post-Secondary Transfer: Applicants with prior credit from a recognized post-secondary institution may satisfy the minimum admission requirements through evaluation of their post-secondary qualifications. Applicants who have completed a Diplóme d'études collégiales (DEC) program may be recognized as post-secondary applicants.

b) Apprentice Applicants

i. Most apprentice programs require applicants to have an employer sponsor and be an active apprentice with SkilledTradesBC.

ii. Applicants must successfully complete each level of apprentice training in sequence to be eligible for progression within their apprenticeship program. Applicants currently enrolled in a level may register for an advanced level prior to completion.

c) Advanced Placement

i. Applicants who have successfully completed academic study at a recognized post-secondary institution or in another BCIT program can apply for Advanced Placement into a program and/or for transfer credit and should consult with the program area prior to application submission.

ii. Admissions will be responsible for the initial evaluation of the program admissions entry requirements. The program area will be responsible for assessing credit equivalency and determining the appropriate entry point. The program area will provide their determination, justification, and completed assessment with appropriate documentation to Admissions (refer to the "Recognition of Prior Learning" process).

iii. Applicants receiving Advanced Placement approval may be given full or partial bulk credit rather than individual course credit.

d) Readmission Applicants

i. Students who interrupt their studies may apply to re-enter their program at a future date. Readmission may depend on seat availability, time elapsed since enrolment, individual circumstances, the successful implementation of a plan resolving previous academic difficulties, suitability of program selection, and other relevant criteria. Readmission to the program is not guaranteed.

ii. Where a program has made significant changes to the learning outcomes since the student last attended, the student may be required to repeat and/or complete additional course work upon readmittance.

iii. Readmission applicants should consult the program area before reapplying. Following program consultation, the application must be submitted to Admissions.

iv. Previously awarded credit through another recognized post-secondary institution or prior learning may be reviewed for recency and relevancy to updated learning outcomes.
v. Program areas will assess applicants for readmission, determine the appropriate re-entry point, and notify Admissions.

e) Applicants through an Education Agreement
   i. Where an applicant applies to a program offered in partnership with another institution or organization, the applicant must satisfy the admission requirements of BCIT and any education agreement requirements.

4 Applicant Residency Status

Application fee is based on applicant residency status at the time of submission.

5 Evaluation Types

a) Alternate Admissions
   i. Applicants who do not meet minimum requirements for admission consideration may have the opportunity to be considered for an alternate admissions process where their previous work experience, non-formal education, cultural knowledge, and other relevant experiences can be used to satisfy admission requirements. Program areas will determine the evaluation criteria or conditions to support alternate admissions to their program.
   ii. In exceptional circumstances, the Associate Dean, in consultation with the subject area expert and the Registrar or designate, may waive one or more of the program admission requirements. The decision is based on an assessment of the applicant's suitability and potential for success in the program.
   iii. Designated Indigenous seats:
      - Indigenous applicants who wish to be considered for designated seats must self-identify as an Indigenous person with membership in, or a family connecting with, a Canadian Indigenous Nation or group, on their application and will be required to present documentation of Indigenous ancestry.
      - Competitive admission programs with designated Indigenous seats will consider all qualified self-identified Indigenous applicants. Indigenous applicants will be assessed alongside the general applicant pool. Indigenous applicants who do not meet the competitive admissions standard will be evaluated for designated Indigenous seats. If applicant demand for designated Indigenous seats is greater than the designated seat allotment, applicants will be ranked.

6 Admissions Communications

The Registrar's Office is BCIT's designated authority for issuing all official admission decisions to applicants.

a) Offers of Admission

i. Applicants must accept their offer of admission within a specified time. Applicants may only accept their offer of admission after the stated acceptance deadline if admission capacity in the program has not yet been reached before the last day to enroll.
ii. Applicants accepted to programs that require it must pay a non-refundable commitment fee to confirm acceptance and secure their seat by the acceptance deadline in their offer letter. Once this fee is received, any outstanding applications will be closed. The non-refundable commitment fee will be applied towards the student's assessed tuition and fees after registration.
iii. BCIT reserves the right to revoke an offer of admission if:
    - BCIT requires a commitment fee and it is not received within the specified time;
    - The student is found to not meet the admissions requirements;
    - The student is found to have violated the Student Code of Conduct or Code of Academic Integrity;
    - The program is cancelled or suspended prior to the start of classes; or,
    - A program intake is cancelled and admission cannot be deferred to a future offering.
iv. It is the applicant's responsibility to notify BCIT of their change in status prior to the start of classes to avoid any unforeseen charges.
v. If the offer of admission is for an international applicant to a program that is eligible for a study permit, BCIT will issue an admission offer letter allowing the applicant to apply for a study permit.

b) Conditional Offer of Admission
i. A conditional offer of admission may be available with program approval.
ii. A conditional offer of admission is granted when an applicant has not yet met all the admission requirements and is accepted upon condition of fulfilling outstanding requirements by a specified date.
iii. A conditional offer of admission will still require a commitment fee if applicable.
iv. Applicants who do not satisfy the conditions of their conditional offer may still be eligible for provisional enrolment, if approved by the Associate Dean, in consultation with the subject matter expert (if applicable), and Admissions. Provisional enrolment may allow a student to enter their program and complete missing admission requirements within their first term. Failure to satisfy the outstanding admissions requirements may result in withdrawal from the program, prevent continuance in the program, and may result in fees paid being non-refundable.

c) Deferred Admission
i. Deferral requests are only considered in extenuating circumstances such as completion of mandatory military service, study permit delays, or other documented circumstances beyond the student's control.
ii. To be eligible for a deferral, applicants must have accepted their offer of full admission, paid their non-refundable commitment fee (if applicable), and have

submitted a deferral request to Admissions thirty days before the program start date. Late applications will be considered on an individual basis.

iii. Applicants offered admission to a graduate or undergraduate level program may request a deferral to that program for a maximum of 2 semesters, subject to program availability.

iv. Any deferral request will require Associate Dean and Associate Registrar approval.

v. Approved deferrals confirm admission to the deferral term, provided the applicant meets any conditions specified in the deferral agreement. If admission requirements change, it is the applicant's responsibility to ensure current requirements are met.

vi. Deferral requests may be denied if the program admission requirements are under review and expected to change for the next admissions cycle.

vii. Attendance at another post-secondary institution may invalidate an approved deferral.

d) Refusal Notice

i. Applicants who are refused admission will receive a refusal notice and are free to re-apply in future without prejudice.

ii. Applications missing admissions requirements are considered incomplete. An applicant will have thirty days, or until final application deadline date, whichever is earlier, to confirm satisfactory completion or in-progress requirements before receiving a refusal notice.

e) Admissions Waitlist Notice

i. Applicants can apply to waitlisted programs if applicable.

ii. Applicants may choose to remain on the waitlist while being assessed for their second-choice program.

iii. Waitlists are dynamic and are subject to change. Waitlisted applicants will not be notified of their place on the waitlist.

iv. Waitlisted applicants will receive offers of admission on an ongoing basis as capacity becomes available up to the last day to enroll. Applicants may be given short notice to accept their offer of admission, pay tuition and fees, and start the program.

v. Waitlisted applicants who decline or do not respond to their offer of admission within the specified time may request to be reinstated on the waitlist. Reinstatement on the waitlist will not guarantee their previous place on the waitlist.

7 Admission Requirements Review and Changes

Changes to admission requirements will not normally be made after an application cycle has begun and must follow Education Council change requirements.

8 Appeal of Admissions Decision

a) An applicant may request the Registrar, or delegate, to review an admission decision if they believe that a procedural error was made in their application evaluation. The

student must submit an Admissions Appeal Form to the Registrar's Office within 10 business days of their application notice of decision. The applicant must provide evidence that a procedural error has happened, meaning a BCIT policy or procedure was violated or misapplied.

b) The decision of the Registrar, or delegate, on an admission appeal will be final.

9 Application and Admissions Misconduct

a) Any person who believes an applicant has violated the Student Code of Conduct (Policy 5102) or Student Code of Academic Integrity (Policy 5104), including plagiarising or submitting fraudulent documents, should report the suspected violation to Admissions.

b) Upon receiving a report of an alleged violation, Admissions will conduct an initial assessment to determine the validity of the alleged violation and provide the findings to the Registrar or delegate.

c) The Registrar or delegate will:
   i. Utilizing principles of judicial fairness, conduct an investigation as per the investigation procedures in Policy 5102 (Student Code of Conduct);
   ii. Make findings of fact based on a balance of probabilities and determine whether a violation occurred;
   iii. Consider relevant contextual factors when determining if a sanction is to be imposed and if so, what the sanction shall be;
   iv. Notify the applicant of the findings, sanction(s) imposed, and appeal process.

d) Consequences of application and admissions misconduct include but are not limited to: revocation of the admission offer, retention of the non-refundable commitment fee and application fee, cancellation of application, prohibition from applying to BCIT for a specified time, or a written warning.

e) If falsified documentation or misrepresentation is discovered after a student's admission, the student may be withdrawn from their program. In cases where the applicant is already registered as a student, the Registrar or delegate may opt to refer the matter to the Senior Director of Student Success or delegate.

Recognition of Prior Learning Procedure

10 Recognition of Prior Learning

a) Applicants and students are responsible for considering the impact of credit for prior learning on all aspects of their student status as it may result in reduced course load (e.g., tuition fees and eligibility for student assistance and awards, study permit eligibility, and post-graduate work permit).

b) Programs can establish specific criteria for transferring credits into their program. These criteria may include recency, a minimum grade needed, and a maximum number of credits allowed to be transferred into the program.

c) Students are responsible for submitting official transcripts and detailed course outlines including course name, course number, length of instructional period, hours per week (lecture, lab, seminar), learning outcomes, course content, required textbooks and readings, methods of instruction, evaluation criterion, and additional relevant details.

d) Academic transcripts completed outside of Canada require a comprehensive international credential evaluation by a member of the Alliance of Credential Evaluation Services of Canada.

10.1 Prior Learning Assessment and Recognition (PLAR) Responsibilities

a) PLAR Application
   i. Applicants and students who believe their learning in other academic, non-academic, or informal learning settings is equivalent to BCIT courses or program learning outcomes may apply for their experience to be assessed toward program admission requirements or course credit ("PLAR"). If applicants or students are only presenting academic history, they will be referred to follow the "Transfer Credit" procedure.
   ii. Applicants and students are responsible for contacting the program area and requesting information about PLAR availability and process.
   iii. Students must pay a non-refundable PLAR assessment fee prior to assessment.
   iv. Some BCIT course credits are not eligible for PLAR credit.
   v. Applicants and students who have received a failing grade in a course shall not be permitted to re-try the failed course through PLAR for one year following the conclusion of the term in which the failure was recorded.

b) PLAR Evaluation
   i. Credit is not guaranteed and is dependent on the assessment results.
   ii. The Assessor is responsible for informing the student of the PLAR process and requirements. The Assessor is responsible for determining whether student documentation supports the claim for credit.
   iii. The Associate Dean has the final approval on PLAR credit and will notify the student of assessment results.
   iv. The Associate Dean or Assessor will notify the Registrar's Office of assessment outcomes.
   v. PLAR credit granted by BCIT may not be recognized by other post-secondary institutions.
   vi. Several evaluation methods are employed during PLAR assessments, which may include, but are not limited to, challenge examinations, skill demonstrations, assignments, interviews, portfolios, and additional documentation to verify competency.
   vii. All credit awarded must be equivalent to an academically recognized course. Unsuccessful PLAR assessments are not recorded on a student transcript.

10.2 Transfer Credit Responsibilities

a) Transfer Credit Application
   i. Only courses with a passing grade or higher can be considered for transfer credit.
   ii. Transfer credits may be granted in recognition of coursework completed at other post-secondary institutions. The courses must have equivalent learning outcomes.

iii. Applicants who have completed substantial equivalency are encouraged to apply for Advanced Placement.
iv. Students applying for transfer credit must submit their transfer credit application and all required documents at least 14 days before term start. Late applications may be accepted only with written authorization from the Associate Dean. BCIT will endeavour to post assessed transfer credit prior to refund deadline.
v. Post-secondary credits used to satisfy program admission requirements are not eligible for transfer credit.

b) Transfer Credit Evaluation
   i. The program area will assess transfer credit applications using BCCAT's *Principles and Guidelines for Transfer*.
   ii. Transfer credit applications will be assessed by the program area in consultation with subject matter experts. Transfer credit will be awarded based on the assessment conducted by the program area, considering the content and level, credit weight, academic structure, textbook, grading and assessment type, and applicants' grades achieved while at the sending institution. The program area is responsible for determining course equivalency and providing the evaluation outcome to the Registrar's Office.
   iii. Transfer credit will be awarded as assigned or general credit on the student's transcript.
   iv. Transfer credit is not included in the calculation of BCIT Grade Point Average (GPA) or Cumulative Grade Point Average (CGPA).
   v. Any documentation associated with the assessment will be retained on the student record.

10.3 Multiple Credentials

a) BCIT encourages students to pursue multiple credentials and may, with limits, apply previously earned credits towards new credentials of the same or higher credential level.
b) BCIT aims to provide students with the most expedient path towards completing credentials.
c) Students with credit for required program courses (earned at BCIT in a prior credential) may apply for credit towards their new program or may be required to complete alternative courses to satisfy program requirements. The final decision to recognize prior credit or determine suitable alternative program courses rests with the program area.
   i. Associate Certificates and Industry Partnership Certificates: A maximum of 75% of the credits for an additional credential may be awarded through previously earned BCIT credits, transfer credits, or a combination of the two.
   ii. Certificates and more advanced credentials: A maximum of 50% of the credits for an additional credential may be awarded through previously earned BCIT credits, transfer credits, or a combination of the two.

11 Education Agreements

Outlined below are general guidelines to be used by programs in establishing education agreements. These guidelines are not intended to, nor should they, contradict any formal provincial arrangements.

a) The following will be mutually agreed upon by the other educational institution and BCIT, and will be stated in writing:
   i. The number of students;
   ii. The portion of the program offered in the other educational institution;
   iii. The length of time for which the transfer agreement is valid;
   iv. The deadline for informing BCIT of the number of transfer students;
   v. Cancellation protocols.

b) The following must be taken into consideration when setting up formal transfer agreements:
   i. The number of required graduates;
   ii. The financial impact to BCIT (e.g., BCIT faculty liaison time, workload, and travel costs);
   iii. Concurrence with BCIT residency requirements.

c) The BCIT teaching departments whose courses are to be offered at the other educational institutions will participate in the transfer program planning process.

d) At least once per year BCIT's designated program representatives will initiate a review of the transfer arrangement to:
   i. Update course outlines;
   ii. Determine the number of transfer students;
   iii. Discuss course changes;
   iv. Review transfer students' progress at BCIT;
   v. Review the duration of the transfer agreement;
   vi. Discuss other matters of mutual concern.

e) BCIT and the other educational institutions will exchange course outlines of the complete program and, where appropriate, will provide copies of handouts, examinations, bibliographies, recommended textbooks, etc.

f) Signing of education agreements must align with Signing Authority Policy 2502.

g) A transfer arrangement and subsequent changes are formalized in writing by the Dean and reported for information to Education Council.

h) Upon the cancellation or expiration of a transfer agreement, all intellectual property rights will revert to the originating institution.

i) Students who successfully complete the portion of the program agreed upon between another educational institution and BCIT are guaranteed admission to BCIT for completion of their program.

j) Students who complete some, but not all, of the other educational institution's program may apply for an individual assessment of courses eligible for transfer credit, advanced placement, or bulk transfer. Admission into BCIT will not be assessed under the terms of the education agreement.

Confidentiality

- Confidential information must not be disclosed to unauthorized individuals.
- Any sharing of information must be performed in accordance with legal requirements and institutional policies.

Forms Associated with This Procedure

Admissions Appeal Form

Amendment History

		Approval Date	Status
Created:	Procedure 5003-PR1 version 1	2009 Mar 11	
Revised:	Procedure 5003-PR1 version 2	2012 Jun 6	
Revised:	Procedure 5003-PR1 version 3	2013 Jun 5	
Revised:	Procedure 5003-PR1 version 4	2014 Oct 1	
Revised:	Procedure 5003-PR1 version 5	2024 Feb 27	In Force

Scheduled Review Date

2029 February 27

ADMISSIONS AND RECOGNITION OF PRIOR LEARNING – PROCEDURE #5003-PR1

REDLINE

i. Applicants must accept their offer of admission within a specified time. Applicants may only accept their offer of admission after the stated acceptance deadline if admission capacity in the program has not yet been reached before the last day to enroll.
ii. Applicants accepted to programs that require it must pay a non-refundable commitment fee to confirm acceptance and secure their seat by the acceptance deadline in their offer letter. Once this fee is received, any outstanding applications will be closed. The non-refundable commitment fee will be applied towards the student's assessed tuition and fees after registration.
iii. BCIT reserves the right to revoke an offer of admission if:
    - BCIT requires a commitment fee and it is not received within the specified time;
    - The student is found to not meet the admissions requirements;
    - The student is found to have violated the Student Code of Conduct or Code of Academic Integrity; ~~or~~
    - The program is cancelled or suspended prior to the start of classes; or,~~.~~
    - A program intake is cancelled and admission cannot be deferred to a future offering.
iv. It is the applicant's responsibility to notify BCIT of their change in status prior to the start of classes to avoid any unforeseen charges.
v. If the offer of admission is for an international applicant to a program that is eligible for a study permit, BCIT will issue an admission offer letter allowing the applicant to apply for a study permit.

b) Conditional Offer of Admission
i. A conditional offer of admission may be available with program approval.
ii. A conditional offer of admission is granted when an applicant has not yet met all the admission requirements and is accepted upon condition of fulfilling outstanding requirements by a specified date.
iii. A conditional offer of admission will still require a commitment fee if applicable.
iv. Applicants who do not satisfy the conditions of their conditional offer may still be eligible for provisional enrolment, if approved by the Associate Dean, in consultation with the subject matter expert (if applicable), and Admissions. Provisional enrolment may allow a student to enter their program and complete missing admission requirements within their first term. Failure to satisfy the outstanding admissions requirements may result in withdrawal from the program, prevent continuance in the program, and may result in fees paid being non-refundable.

c) Deferred Admission
i. Deferral requests are only considered in extenuating circumstances such as completion of mandatory military service, study permit delays, or other documented circumstances beyond the student's control.
ii. To be eligible for a deferral, applicants must have accepted their offer of full admission, paid their non-refundable commitment fee (if applicable), and have

DECISION NOTE
November 20, 2025

PREPARED FOR: Board of Governors

PREPARED BY: Shawna Waberi, Chair, Education Council

ISSUE: Recording in the Classroom - Policy #5201 and Recording in the Classroom - Procedure #5201-PR1

APPENDICES:

1. Appendix A: Recording in the Classroom - Policy #5201, draft
2. Appendix B: Recording in the Classroom - Policy #5201, redline
3. Appendix C: Recording in the Classroom - Procedure #5201-PR1, draft
4. Appendix D: Recording in the Classroom - Procedure #5201-PR1, redline

RECOMMENDATION:

THAT the Board of Governors approves the revised *Recording in the Classroom - #5201 and Recording in the Classroom - Procedure #5201-PR1*.

BACKGROUND:

The Recording in the Classroom - Policy #5201 and Procedure #5201-PR1 were last amended in 2020. A scheduled review was completed, and revisions were made. Since 2020, there has been a significant increase in the use of digital tools for classroom recording, especially following the shift to online learning during the COVID-19 pandemic. Emerging technologies such as AI transcription, increased use of third-party platforms, and evolving expectations around Universal Design prompted the need for comprehensive revision. The revised policy was developed to address gaps in the original version, provide clearer guidance around student-initiated and faculty-initiated recording, and align with legislative and institutional policies.

SUMMARY:

Following extensive consultation by the working group and a 30-day community consultation period resulting in further edits, the Education Council (EdCo) Policy Committee endorsed moving the policy and procedure forward to the November 19, 2025, Education Council meeting and request approval from the Board of Governors.

Prior to the EdCo meeting on November 18, the Governance Committee reviewed and recommended approval of the policy and procedure, with a few non-substantial, yet clarifying changes. Updates to the definitions of “recording” and “faculty” in the policy and subsequent replacement of “instructor” with “faculty” in both policy and procedure. Minor updates to language in the procedure for student-initiated recordings improved clarity and flow. These changes were

incorporated into the policy and procedure and approved at the November 19 Education Council meeting.

The following revisions were made:

- Reaffirming faculty discretion for consent to record in the classroom, except where required by law of Accommodation for Students with Disabilities - Policy #4501.
- Explicit prohibition of altering recordings and related media.
- Comprehensive additions to the procedure to clearly outline the process of seeking permission, notification and consent, end-use, and storage of recordings.

RECORDING IN THE CLASSROOM – POLICY #5201

REVISED DRAFT

BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

Recording in the Classroom [Draft revision]

Policy No:	5201
Version:	2
Category:	Education
Approving Body:	Board of Governors (on advice of Education Council)
Executive Sponsor:	Provost and VP Academic
Department Responsible:	Education Council & BCIT Schools
Directory of Records Class:	0650-15
Approval Date:	yyyy mmm dd [tbd]
Effective Date:	2026 January 1

Policy Statement

BCIT recognizes that recording in the classroom can be effective in supporting the student learning experience, and encourages its practice whenever deemed appropriate by faculty.

Except where required by law or approved as an accommodation under Policy 4501, Accommodation for Students with Disabilities, BCIT faculty members have full discretion over whether recording is permitted in their classes.

Accommodation-related recordings are governed by Policy 4501 and managed by BCIT Accessibility Services. Under that process, faculty are notified of an approved accommodation (e.g., recording for note-taking) through the Individual Accommodation Plan (IAP) and Accessibility Services is responsible for communicating any relevant terms and conditions to the student. In such cases, additional faculty permission or class-wide notification is not required.

Under this policy, faculty members may deny a student request to record or approve it subject to reasonable conditions as set out in Procedure 5201-PR1. Any use of recordings beyond the original instructional purpose requires additional written approval. Faculty-initiated recordings for instructional purposes are permitted, with notification and consent handled as set out in Procedure 5201-PR1.

The conduct of a student who has disregarded a faculty member's prohibition or restrictions on recording may be investigated under Policy 5104, Student Code of Academic Integrity and Procedure 5104-PR1, Procedure for Violations of Code of Academic Integrity, and, where applicable, Policy 5102, Student Code of Conduct (Non-Academic).

Purpose of Policy

This policy establishes:

- the circumstances in which students and faculty are permitted to make recordings in the classroom;
- the conduct expected of students and faculty when recording in the classroom;
- the distinction between general student-initiated recordings and student-initiated recordings approved as accommodations;
- clear rules regarding retention, privacy, and distribution of classroom recordings;
- potential consequences of failing to comply with this policy; and,

- the respective duties and responsibilities of students, faculty members, staff, and other BCIT officials in adhering to this policy.

Application of this Policy

This policy applies to all BCIT students, faculty members, guest lecturers, and staff.

Scope

This policy applies to recordings in the classroom, other than when a recording is an accommodation made under Policy 4501, Accommodation for Students with Disabilities.

Related Documents and Legislation

BCIT Policies:

Policy 3501, Acceptable Use of Information Technology
Policy 3502, Information Security
Policy 4501, Accommodation for Students with Disabilities
Policy 5102, Student Code of Conduct (Non-Academic)
Policy 5104, Student Code of Academic Integrity
Policy 6700, Freedom of Information and Protection of Privacy
Policy 6701, Records Management
Policy 7506, Use of Materials Protected by Copyright

Legislation:

College and Institute Act, RSBC 1996, c 52

Definitions

In this policy and all associated procedures:

"accommodation" means a modification or adaptation that is designed to reduce or remove barriers to participation for a Student with a Disability.

"classroom" refers to all learning environments, including face-to-face, blended, laboratory, field, shop, and online.

"faculty member" or **"faculty**" refers to any person hired by BCIT to conduct classroom or teaching activities, as defined in Part 1 of the College and Institute Act, R.S.B.C. 1996, c.52, of the province of British Columbia.

"recording" means the creation of video, images, or audio files (or combinations thereof) that can reproduce course material or presentations by a faculty member, student, guest, or other participant; "recording" does not include the act of physically handwriting or typing notes.

"student" refers to a person who is enrolled in or who has been accepted for enrollment at the Institute in full-time or part-time courses.

"student(s) with a disability" refers to a student who has a condition that is recognized as a mental or physical disability under the BC Human Rights Code and who is therefore protected from discrimination based on this condition.

Student-Initiated Recordings

Student learning and development may benefit from being able to record lectures, classroom activities, and materials used in the classroom. Students without an approved accommodation must request permission from faculty to make recordings in the classroom.

Written permission must be obtained from the faculty member prior to recording. Written permission shall be retained by the faculty member and the student; it should include the date or dates of recording, the purpose of the recording, the method of recording, and the intended method of storage.

Student-initiated recording is permitted only for the purposes of private study by the individual students to whom permission was granted. Students may not post, email, upload to third-party platforms, distribute or otherwise communicate these materials without additional written permission from the faculty member.

Students making approved recordings must not capture the images or voices of other students who have not consented to being recorded. Faculty members may place reasonable conditions on the method or extent of recording to protect student privacy and maintain a constructive classroom environment.

Permission to make a recording does not constitute a license or assignment of any copyright in the recorded material. See Policy 7506, Use of Materials Protected by Copyright, for BCIT's rules regarding copyrighted material.

Prohibited conduct includes unauthorized distribution, synthetic or deceptive alteration of recordings (e.g., AI-based manipulation), or use that misrepresents what occurred in class.

Student contravening this Policy or any of its Procedures may be subject to discipline under Policy 5102, Student Code of Conduct (Non-Academic) and Policy 5104, Student Code of Academic Integrity.

Faculty-Initiated Recording for Instructional Purposes

Faculty may record classroom activities for educational purposes as part of their instructional methods or curriculum. This includes lecture, lab, and seminar capture; demonstrations; group discussions; or other activities supporting course learning outcomes. Classroom activities may take place in physical classrooms and laboratories, virtual environments, or other instructional settings, including field locations or public learning spaces.

In such cases, the faculty member must provide notice to students prior to the recording taking place, including the purpose of the recording, how it will be used, and who will have access (as outlined in Procedure 5201-PR1, Recording in the Classroom).

For regularly scheduled recordings that are part of instructional design or curriculum, such as mandatory lecture capture, this notice should be included in the course outline. For ad hoc or incidental recordings, the faculty member must notify students in advance and provide the same information, either verbally or via the Learning Hub.

If a classroom recording captures identifiable information of students or other individuals such as guest speakers, volunteers, or community members, the faculty member must obtain informed consent (as outlined in Procedure 5201-PR1).

Recordings must be stored on BCIT-approved platforms and retained in accordance with institutional records management policies and privacy obligations. Recordings used for grading or academic decisions must be retained for a minimum of one year from the date the decision is made, in accordance with Policy 6700. Recordings used for general learning or review purposes should follow standard course content retention timelines.

Sensitive Classroom Discussions

As outlined in Procedure 5201-PR1, Recording in the Classroom, faculty members may temporarily pause or prohibit recording or ask students to refrain from notetaking during classroom activities that involve sensitive discussion or self-disclosure. This discretion supports a respectful and inclusive learning environment and ensures alignment of recording practices and BCIT's values of privacy, academic integrity, and student well-being.

Procedures Associated with This Policy

Procedure 5201-PR1, Recording in the Classroom

Forms Associated with This Policy

None

Amendment History

			Approval Date	Status
1.	Creation:	Policy 5201 version 1	2020 MAY 26	In Force
2.	Revised:	Policy 5201 version 2 [draft]	tbd	pending approval

Scheduled Review Date

[tbd] Five years from date of approval, or earlier if required due to operational or regulatory changes.

RECORDING IN THE CLASSROOM – POLICY #5201

REDLINE

Recording in the Classroom [Draft revision]

Policy No:	5201
Version:	~~1~~2
Category:	Education
Approving Body:	Board of Governors (on advice of Education Council)
Executive Sponsor:	~~Chair of Education Council~~Provost and VP Academic
Department Responsible:	Education Council & BCIT Schools
Directory of Records Class:	0650-15
Approval Date:	yyyy mmm dd [tbd]~~2020 MAY 26~~
Effective Date:	2026 January 1

Policy Statement

BCIT recognizes that recording in the classroom can be effective in supporting the student learning experience ~~for students~~, and encourages its practice whenever deemed appropriate by faculty.

Except where required by law or approved as an accommodation under Policy 4501, Accommodation for Students with Disabilities, BCIT faculty members ~~have responsibility for classroom management, and~~ have full discretion over whether recording is permitted ~~or prohibited~~ in their classes~~, except where recording is part of accommodating a student with a disability under Policy 4501, Accommodation for Students with Disabilities.~~.

Accommodation-related recordings are governed by Policy 4501 and managed by BCIT Accessibility Services. Under that process, ~~instructors~~ faculty are notified of an approved accommodation (e.g., recording for note-taking) through the Individual Accommodation Plan (IAP) and Accessibility Services is responsible for communicating any relevant terms and conditions to the student. In such cases, additional ~~instructor~~faculty permission or class-wide notification is not required.

Under this policy, faculty members may deny a student request to record or approve it subject to reasonable conditions as set out in Procedure 5201-PR1. Any use of recordings beyond the original instructional purpose requires additional written approval. Faculty-initiated recordings for instructional purposes are permitted, with notification and consent handled as set out in Procedure 5201-PR1.~~Faculty members may choose to approve recording all classroom activities or specific parts of their instruction, by providing prior written permission that sets out what may be recorded, how such recordings may be used and/or shared between students, and any limits the faculty member wishes to impose.~~

The conduct of a student who has disregarded ~~an instructor's~~a faculty member's prohibition or restrictions on recording may be investigated under Policy 5104, Student Code of Academic Integrity and Procedure 5104-PR1, Procedure for Violations of Code of Academic Integrity, and, where applicable, Policy 5102, Student Code of Conduct (Non-Academic).

~~Any student who disregards a faculty member's prohibition or restrictions on recording may be sanctioned for academic misconduct under Policy 5104, Student Code of Academic Integrity.~~

Purpose of Policy

This policy establishes:

- the circumstances in which students and ~~instructors~~faculty are permitted to make recordings in the classroom;
- the ~~behaviours, attitudes and general~~ conduct expected of students and ~~instructors~~faculty when ~~making permitted~~ recording~~s~~ in the classroom;
- the distinction between general student-initiated recordings and student-initiated recordings approved as accommodations;
- clear rules regarding retention, privacy, and distribution of classroom recordings;
- potential consequences of failing to comply with this policy; and,
- the respective duties and responsibilities of students, faculty members, staff, and other BCIT officials in adhering to this policy.

Application of this Policy

This policy applies to all BCIT students, faculty members, guest lecturers, and staff.

Scope

This policy applies to recordings in the classroom, other than when a recording is an accommodation made under Policy 4501, Accommodation for Students with Disabilities.

Related Documents and Legislation

BCIT Policies:

Policy 3501, Acceptable Use of Information Technology
Policy 3502, Information Security
~~BCIT~~ Policy 4501, Accommodation for Students with Disabilities
~~BCIT Policy 5100, Glossary of Educational Policy Terms~~
~~BCIT~~ Policy 5102, Student Code of Conduct (Non-Academic)
~~BCIT~~ Policy 5104, Student Code of Academic Integrity
Policy 6700, Freedom of Information and Protection of Privacy
Policy 6701, Records Management
Policy 7506, Use of Materials Protected by Copyright

~~BCGEU Collective Agreement~~
~~**FSA Collective Agreement**~~**Legislation:**

College and Institute Act, RSBC 1996, c 52
~~*Copyright Act*, RSC 1985, c C-42~~

Definitions

~~All terms and language used in this document are consistent with Policy 5100, Glossary of Educational Policy terms.~~

In this policy and all associated procedures:

"**accommodation**" means a modification or adaptation that is designed to reduce or remove barriers to participation for a Student with a Disability.

"**classroom**" refers to all learning environments, including face-to-face, blended, laboratory, field, shop, and online.

"faculty member" or "~~**instructor**~~**faculty**" refers to any person hired by BCIT to conduct classroom or teaching activities, as defined in Part 1 of the College and Institute Act, R.S.B.C. 1996, c.52, of the province of British Columbia.

"**recording**" means the creation of video, images, or audio files (or combinations thereof) that can reproduce ~~fixation in any form, whether electronic or otherwise, of course material~~classroom content ~~or presentations~~ ~~presented~~ by a faculty member, student, guest, or other participant~~, including the creation of video, image, or audio files that can reproduce course materials~~; "recording" does not include the act of physically handwriting or typing notes~~; and~~.

~~"**classroom**" refers to all learning environments, including face-to-face, blended, laboratory, field, shop, and online.~~

"student" refers to a person who is enrolled in or who has been accepted for enrollment at the Institute in full-time or part-time courses.

"**student(s) with a disability**" refers to a student who has a condition that is recognized as a mental or physical disability under the BC Human Rights Code and who is therefore protected from discrimination based on this condition.

~~Recording for Private Study~~ ~~(~~Student-Initiated Recordings~~)~~

Student~~s~~ learning and development may benefit from being able to record lectures, classroom activities, and materials used in the classroom. Students without an approved accommodation ~~may~~ must request permission from a faculty member to make recordings in the classroom ~~in order to support their learning and development~~.

Written permission must be obtained from the faculty member prior to recording~~Permission is required from the faculty member prior to engaging in recording or copying classroom activities, as per Procedure 5201-PR1, Recording in the Classroom.~~. ~~——~~Written permission shall be retained by the faculty member and the student; it should include the date or dates of recording, the purpose of the recording, the method of recording, and the intended method of storage.~~Written permission shall be retained by the faculty member and the student.~~

~~Any faculty approved~~ Student-initiated recording is permitted only for the purposes of private study by the individual students to whom permission was granted. ~~that individual studen~~Students may not post, email, upload to third-party platforms, ~~t, who may not~~ distribute ~~,~~

~~email~~ or otherwise communicate these materials ~~to any other person~~ without additional ~~additional specific~~ written permission from the ~~instructor~~faculty ~~to do so from the faculty member~~.

Students making approved recordings must ~~be respectful and ensure a constructive learning environment, including~~ not ~~making all reasonable efforts to avoid~~ capturinge the images or voices of other students who have not consented to being recorded~~do not want to be recorded~~. Faculty members may place reasonable conditions on the method or extent of recording to protect student privacy and maintain a constructive classroom environment.

Permission to make a recording does not constitute a license or assignment of any copyright in the recorded material. See Policy 7506, Use of Materials Protected by Copyright, for BCIT's rules regarding copyrighted material.

Prohibited conduct includes unauthorized distribution, synthetic or deceptive alteration of recordings (e.g., AI-based manipulation), or use that misrepresents what occurred in class.

~~A s~~Student ~~who contravenes~~ contravening this Policy or any of its ~~associated~~ Procedures may be subject to discipline under Policy 5102, Student Code of Conduct (Non-Academic) and~~/or~~ Policy 5104, Student Code of Academic Integrity.

~~Permission to make a recording does not constitute a license or assignment of any copyright in the recorded material. See Policy 7506, Use of Materials Protected by Copyright, for BCIT's rules regarding copyrighted material.~~

Faculty-Initiated Recording for Instructional Purposes

Faculty may record classroom activities for educational purposes as part of their instructional methods or curriculum. This includes lecture, lab, and seminar capture; demonstrations; group discussions; or other activities supporting course learning outcomes. Classroom activities may take place in physical classrooms and laboratories, virtual environments, or other instructional settings, including field locations or public learning spaces.~~require students to participate in classroom activities that are recorded as part of their instructional methods and/or curriculum, including (but not limited to) webinar sessions and lecture capture.~~

In such cases, the ~~instructor~~faculty member must provide notice to students prior to the recording taking place, including the purpose of the recording, how it will be used, and who will have access (as outlined in Procedure 5201-PR1, Recording in the Classroom).

For regularly scheduled recordings that are part of instructional design or curriculum, such as mandatory lecture capture, this notice should be included in the course outline. For ad hoc or incidental recordings, the faculty member must notify students in advance and provide the same information, either verbally or via the Learning Hub.

If a classroom recording captures identifiable information of students or other individuals such as guest speakers, volunteers, or community members, the faculty member must obtain informed consent (as outlined in Procedure 5201-PR1).

Recordings must be stored on BCIT-approved platforms and retained in accordance with institutional records management policies and privacy obligations. Recordings used for grading or academic decisions must be retained for a minimum of one year from the date the decision is made, in accordance with Policy 6700. Recordings used for general learning or review purposes should follow standard course content retention timelines.

Sensitive Classroom Discussions

As outlined in Procedure 5201-PR1, Recording in the Classroom, ~~instructors~~faculty members may temporarily pause or prohibit recording or ask students to refrain from notetaking during classroom activities that involve sensitive discussion or self-disclosure. This discretion supports a respectful and inclusive learning environment and ensures alignment of recording practices and BCIT's values of privacy, academic integrity, and student well-being.

~~In such cases, the faculty member must provide advance notification to students that their classroom activities will be recorded, by including a notification and description of the recording requirements in the course outline, as per Procedure 5201-PR1, Recording in the Classroom.~~

~~Scope~~

~~This policy applies to recordings in the classroom, other than when a recording is an accommodation made under Policy 4501, Accommodation for Students with Disabilities.~~

Procedures Associated ~~With~~with This Policy

Procedure 5201-PR1, Recording in the Classroom

Forms Associated ~~With~~with This Policy

None

Amendment History

		Approval Date	Status
1.	Creation: Policy 5201 version 1	2020 MAY 26	In Force
~~1.~~2.	Revised: Policy 5201 version 2 [draft]	tbd	pending approval

Scheduled Review Date

[tbd] Five years from date of approval, or earlier if required due to operational or regulatory changes. ~~2022 May 26~~

RECORDING IN THE CLASSROOM – PROCEDURE #5201-PR1

REVISED DRAFT

BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

Recording in the Classroom [Draft revision]

Procedure No:	5201-PR1
Version:	2
Applicable Policy:	5201, Recording in the Classroom
Category:	Education
Approving Body:	Board of Governors (on advice of Education Council)
Executive Sponsor:	Provost and VP Academic
Department Responsible:	Education Council & BCIT Schools
Directory of Records Class:	0650-15
Approval Date:	yyyy mmm dd [tbd]
Effective Date:	2026 January 1

Objectives

This procedure describes how students may seek permission to make recordings in the classroom and create a record of such permission, and details the requirements that apply to faculty wishing to record in the classroom for instructional purposes.

This procedure does not limit a student's right to record classroom content as part of an approved accommodation under Policy 4501, Accommodation for Students with Disabilities. However, accommodated students must meet BCIT's expectations around respectful learning, privacy, and data handling.

Application

This procedure applies to all BCIT students, faculty, guest lecturers, and staff.

Procedure

Student-Initiated Recordings

A student (or group of students) wishing to record classroom activities must request written permission directly from the faculty member prior to any recording taking place. Securing permission for recording in the classroom may be initiated by students, or by the faculty member.

Written permission must include:

- course name and registration number;
- name (names) of the student (students) authorized to record;
- start and end dates of the approved recording period;
- purpose of the recording;
- method of recording (e.g., audio only, video); and,
- intended method of storage (e.g., local drive, BCIT cloud storage).

Faculty members approving recording in the classroom may provide written permission by email, by written notice online in the Learning Hub, or by indicating permission in the course outline. Written permission shall be retained by both the faculty member and the students to verify permission has been sought and obtained.

For student-initiated recordings not governed by Policy 4501, faculty members may deny a request to record, approve the recording of all classroom activities, or grant approval subject to reasonable conditions. Reasonable conditions may specify what is recorded, how recordings are made, where they are stored, how they may be used and shared among students, and when they must be deleted. Students must comply with all conditions and must not record identifiable images or audio of other students without their consent.

Students must use approved recordings only for the purpose of private study and may not distribute, post, or share them without further written permission from the faculty member. Prohibited conduct includes synthetic or deceptive alteration of recordings (e.g., AI-based manipulation) or any use that misrepresents what occurred in class. Unauthorized recording or misuse may be investigated under Policy 5104, Student Code of Academic Integrity and Procedure 5104-PR1, Procedure for Violations of Code of Academic Integrity, and, where applicable, Policy 5102, Student Code of Conduct (Non-Academic).

Faculty-Initiated Recordings for Instructional Purposes

Where faculty members require students to participate in classroom activities that are recorded as part of their instructional methods or curriculum (including webinar sessions, lab or lecture capture) they must give notice to students before recording begins.

For regularly scheduled recordings (e.g., ongoing lecture or seminar capture), notice:

- must be included in the course outline;
- should specify the purpose of the recording, how it will be used, and who will have access.

For ad hoc or incidental recordings (e.g., guest speakers, special sessions):

- the same information must be provided verbally or in writing (e.g., via the Learning Hub) prior to recording;
- best practice is to provide written notification where feasible.

All faculty-initiated recordings must be stored on BCIT-approved platforms with the following retention guidelines:

- recordings used for grading or academic decisions must be retained for at least one year from the date of the decision, in accordance with Policy 6700 and BCIT's retention schedule;
- recordings used for general learning or review purposes (e.g., lecture reference) should be retained for the same duration as course content.

Notification and Consent of Students and Third Parties

When classroom recordings capture identifiable images, audio, or personal information of faculty, students or third parties, faculty members must ensure individuals are informed in advance and consent is managed appropriately.

Student Participation in Recordings:

- Advance notice must be provided to students when a recording will take place. Notification should include the purpose of the recording, how it will be used, who will have access, and where it will be stored.

- In physical classrooms, students should be given the option to sit outside the recording frame and not verbally participate where possible.
- In online environments, students should be informed that they may turn off their cameras or microphones if they do not wish to appear in the recording.

Faculty Use Beyond the Course:

- Student consent is not required if the recording is:
  - used only for instructional purposes;
  - shared only with students enrolled in the same course section; and
  - made accessible only through BCIT's Learning Hub or other approved platform.
- If a recording will be used beyond its original instructional purpose (e.g., shared with future classes, other cohorts, or made publicly available on platforms such as YouTube), any identifiable students or third parties must provide written informed consent using a BCIT-approved consent form.
- If consent is not provided, individuals' image and voice must be obscured or removed before the recording is reused or distributed.

Withdrawing Consent:
Individuals who have consented to their recorded image or voices being reused outside the instructional purpose may withdraw consent at any time before publication or redistribution. Once a recording has been published or shared externally, BCIT will make reasonable efforts to remove the content where feasible but cannot guarantee full retraction from third-party platforms.

Sensitive Classroom Discussions and Pausing Recordings
A faculty member may pause or prohibit recording and/or ask students to refrain from notetaking during classroom discussions that involve sensitive topics or personal self-disclosure. Sensitive discussions may include, but are not limited to:

- sharing of personal experiences related to health, identity, trauma, family, or lived experience;
- discussions involving ethical dilemmas, professional boundaries, or personal reflection;
- group conversations that rely on mutual trust or confidentiality (e.g., counselling or health programs); and,
- dialogue intended to foster empathy, perspective-taking, or critical discussion of lived realities.

In such cases, the faculty member should ask all students to put their pens down, stop typing, and turn off audio or video recordings. Faculty are encouraged to clearly communicate when and why recording or notetaking is paused and to provide alternative summaries or instructional materials where appropriate to support learning continuity.

Related Documents and Legislation

As cited in the Policy.

Amendment History

			Approval Date	Status
1.	Creation:	Procedure 5201-PR1 version 1	2020 MAY 26	In Force
2.	Revised:	Procedure 5201-PR1 [draft] version 2	yyyy mmm dd	pending approval

Scheduled Review Date

[tbd] Five years from date of approval, or earlier if required due to operational or regulatory changes

RECORDING IN THE CLASSROOM – PROCEDURE #5201-PR1

REDLINE

BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

Procedure

Recording in the Classroom [Draft revision]

Procedure No:	5201-PR1
Version:	~~1~~2
Applicable Policy:	5201, Recording in the Classroom
Category:	Education
Approving Body:	Board of Governors (on advice of Education Council)
Executive Sponsor:	Provost and VP Academic~~Chair of Education Council~~
Department Responsible:	Education Council & BCIT Schools~~Education~~
Directory of Records Class:	0650-15
Approval Date:	yyyy mmm dd [tbd]~~2020 MAY 26~~
Effective Date:	2026 January 1

Objectives

This procedure describes ~~the process by which~~how students may seek permission to make recordings in the classroom and ~~,~~ creat~~ing~~te a record of such permission, and ~~providing~~ details ~~of~~ the requirements that apply to faculty ~~who~~ wish~~ing~~ to record in the classroom for instructional purposes.

This procedure does not limit a student's right to record classroom content as part of an approved accommodation under Policy 4501, Accommodation for Students with Disabilities. However, accommodated students must meet BCIT's expectations around respectful learning, privacy, and data handling. ~~This procedure does not apply to any student with a disability who is registered with Accessibility Services and requires recordings of course material as an accommodation.~~

~~Who Does This Procedure Apply To?~~Application

This procedure applies to all BCIT students, faculty, guest lecturers, and staff.

Procedure

Student-Initiated Recordings~~Obtaining Permission from a Faculty Member~~

A student (or group of students) wishing~~seeking permission for recording in the~~to record classroom activities must request written permission directly from the faculty member prior to any recording taking place. Securing p~~P~~ermission for recording in the classroom may be initiated by ~~the party seeking permission~~students, or ~~proactively~~ by the faculty member.

Written permission must include:

- course name and registration number;
- name (names) of the student (students) authorized to record;
- start and end dates of the approved recording period;
- purpose of the recording;
- method of recording (e.g., audio only, video); and,
- intended method of storage (e.g., local drive, BCIT cloud storage).

~~Instructors~~Faculty members approving recording in the classroom may provide written permission by email, by written notice online in the Learning Hub, or by indicating permission in the course outline. ~~Faculty who approve of recording in the classroom may provide written permission by email, by written notice online in the Learning Hub, or by specifically indicating permission in the course outline. Written permission should include the name of the course, the name of approved students (or identify the entire class as approved), and the start and end dates for which recording has been approved.~~

Written permission shall be retained by both the faculty member and the student~~(s), in order to demonstrate that~~s to verify permission has been sought and obtained.

For student-initiated recordings not governed by Policy 4501, faculty members may deny a request to record, ~~to~~ approve the~~a~~ recording of all classroom activities, or ~~to approve it~~ grant approval subject to reasonable conditions. Reasonable conditions may specify what is recorded, how recordings are made, where they are stored, how they may be used and shared among students, and when they must be deleted. Students must comply with all conditions and must not record identifiable images or audio of other students without their consent.

Students must use approved recordings only for the purpose of private study and may not distribute, post, or share them without further written permission from the faculty member. Prohibited conduct includes synthetic or deceptive alteration of recordings (e.g., AI-based manipulation) or any use that misrepresents what occurred in class. Unauthorized recording or misuse may be investigated under Policy 5104, Student Code of Academic Integrity and Procedure 5104-PR1, Procedure for Violations of Code of Academic Integrity, and, where applicable, Policy 5102, Student Code of Conduct (Non-Academic).

Faculty-Initiated Recordings for Instructional Purposes~~**Faculty Members Using Recording for Instructional Purposes or Curriculum**~~

~~In cases when~~ Where faculty members require students to participate in classroom activities that are recorded as part of their instructional methods ~~and/~~or curriculum (including webinar sessions, lab or lecture capture~~, etc~~) they ~~, faculty~~ must give notice to students before recording begins.~~include a notification in the course outline identifying the recording requirement.~~

For regularly scheduled recordings (e.g., ongoing lecture or seminar capture), notice:

- must be included in the course outline;
- should specify the purpose of the recording, how it will be used, and who will have access.

For ad hoc or incidental recordings (e.g., guest speakers, special sessions):

- the same information must be provided verbally or in writing (e.g., via the Learning Hub) prior to recording;
- best practice is to provide written notification where feasible.

All faculty-initiated recordings must be stored on BCIT-approved platforms with the following retention guidelines:

- recordings used for grading or academic decisions must be retained for at least one year from the date of the decision, in accordance with Policy 6700 and BCIT's retention schedule;
- recordings used for general learning or review purposes (e.g., lecture reference) should be retained for the same duration as course content.

Notification and Consent of Students and Third Parties

When classroom recordings capture identifiable images, audio, or personal information of ~~instructors~~faculty, students or third parties, faculty members must ensure individuals are informed in advance and consent is managed appropriately.

Student Participation in Recordings:

- Advance notice must be provided to students when a recording will take place. Notification should include the purpose of the recording, how it will be used, who will have access, and where it will be stored.
- In physical classrooms, students should be given the option to sit outside the recording frame and not verbally participate where possible.
- In online environments, students should be informed that they may turn off their cameras or microphones if they do not wish to appear in the recording.

~~Instructor~~Faculty Use Beyond the Course:

- Student consent is not required if the recording is:
  - used only for instructional purposes;
  - shared only with students enrolled in the same course section; and
  - made accessible only through BCIT's Learning Hub or other approved platform.
- If a recording will be used beyond its original instructional purpose (e.g., shared with future classes, other cohorts, or made publicly available on platforms such as YouTube), any identifiable students or third parties must provide written informed consent using a BCIT-approved consent form.
- If consent is not provided, individuals' image and voice must be obscured or removed before the recording is reused or distributed.

Withdrawing Consent:

Individuals who have consented to their recorded image or voices being reused outside the instructional purpose may withdraw consent at any time before publication or redistribution. Once a recording has been published or shared externally, BCIT will make reasonable efforts to remove the content where feasible but cannot guarantee full retraction from third-party platforms.

Sensitive Classroom Discussions and Pausing Recordings

A faculty member may pause or prohibit recording and/or ask students to refrain from notetaking during classroom discussions that involve sensitive topics or personal self-disclosure. Sensitive discussions may include, but are not limited to:

- sharing of personal experiences related to health, identity, trauma, family, or lived experience;
- discussions involving ethical dilemmas, professional boundaries, or personal reflection;
- group conversations that rely on mutual trust or confidentiality (e.g., counselling or health programs); and,
- dialogue intended to foster empathy, perspective-taking, or critical discussion of lived realities.

In such cases, the faculty member should ask all students to put their pens down, stop typing, and turn off audio or video recordings. Faculty are encouraged to clearly communicate when and why recording or notetaking is paused and to provide alternative summaries or instructional materials where appropriate to support learning continuity.

Related Documents and Legislation

As cited in the Policy.

- ~~BCIT Policy 4501, Accommodation for Students with Disabilities~~
- ~~BCIT Policy 5100, Glossary of Educational Policy Terms~~
- ~~BCIT Policy 5102, Student Code of Conduct (Non-Academic)~~

~~BCIT Policy 5104, Student Code of Academic Integrity~~

- ~~BCGEU Collective Agreement~~
- ~~FSA Collective Agreement~~
- ~~*College and Institute Act*, RSBC 1996, c 52~~
- ~~*Copyright Act*, RSC 1985, c C-42~~

Amendment History

		Approval Date	Status
1. Creation:	Procedure 5201-PR1 version 1	2020 MAY 26	In Force
~~1.~~2. Revised:	Procedure 5201-PR1 [draft] version 2	yyyy mmm dd	pending approval

Scheduled Review Date

[tbd] Five years from date of approval, or earlier if required due to operational or regulatory changes~~2022 May 26~~

DECISION NOTE
November 20, 2025

PREPARED FOR: Human Resources Committee

PREPARED BY: Chris Hudson, VP, People, Culture & Inclusion
Tanya Buschau, Advisor, Respect, Diversity & Inclusion

ISSUE: Prevention of Discrimination, Harassment, and Bullying – Policy #7507, and Harassment and Discrimination – Procedures #7507-PR1

APPENDICES:

1. Appendix A: Prevention of Discrimination, Harassment, and Bullying – Policy #7507, draft
2. Appendix B: Harassment and Discrimination – Policy #7507, redline
3. Appendix C: Prevention of Discrimination, Harassment, and Bullying – Procedure #7507-PR1, draft
4. Appendix D: Harassment and Discrimination – Procedure #7507-PR1, redline

RECOMMENDATION:

THAT the Board of Governors approves the revised *Prevention of Discrimination, Harassment, and Bullying - Policy #7507, and Procedure #7507-PR1*, with the provision that it shall come into effect on January 5, 2026.

BACKGROUND:

The Human Resources Committee approved the revised policy for recommendation at their November 18, 2025 meeting.

The current policy and procedures were last updated in 2014. They were not previously approved by the Board of Governors, but by the leadership team.

As per the current 2014 policy and procedures:

13. Steering Committee

There shall be a steering committee comprising members representing the parties to this policy. The steering committee shall provide interpretation of this policy and shall be responsible for any revisions to the Policy and Procedure 7507-PR1. The committee shall meet at least quarterly and more often if requested by members of the committee. The Advisor shall be a resource to the steering committee.

14. Period Review of Policy and Procedures

This Policy 7507 and Procedure 7507-PR1 are ratified for a three-year period by BCIT, the BCGEU Local 703 Support Staff and Instructional Bargaining Units, the BCIT Faculty and Staff Association,

and the Student Association.

During this time, amendments or revisions to the policy or the procedures may be made by mutual agreement of the parties. A formal review of the policy will be conducted annually. Any renewal or revision of this agreement must be mutually agreed to by all the parties to the agreement.

Development Process:

The Harassment and Discrimination Steering Committee, supported by the Respect, Diversity & Inclusion (RDI) team has worked diligently to create an updated draft policy and procedure. Unlike other BCIT policies, all revisions require agreement from all parties (i.e. BCIT, the three employee unions, and the Student Association). It has taken a significant amount of time to create the revised drafts. This process included seeking feedback from the policy management team, legal counsel, and a 45-day community consultation, involving additional review and revision by the Harassment and Discrimination Steering Committee.

All Harassment and Discrimination Steering Committee members tentatively agreed the revised drafts that were returned to the Policy Review Team in August 2025 with the sponsor requesting endorsement to the Board of Governors after the completion of the union and association approval. Each of the Steering Committee members have confirmed, on behalf of their respective unions or associations, that these drafts are approved by them.

Summary of Notable Changes:

The current policy and procedures apply to students, employees and contract employees whereas the revisions expand the application to “all BCIT students, employees, contractors, volunteers, visitors, and members of the Board of Governors, during all BCIT-related activities.”

Although the policy and procedures have been extensively revised, aside from the noted change, most updates are simply clarifications of previously unclear sections.

What is considered prohibited conduct under the current Policy has not been substantively changed, i.e., the Policy still prohibits bullying, harassment, and discrimination. However, definitions have been added and amended primarily to provide clarity (not to expand nor diminish the scope of what actions or comments would violate the policy). Changes to definitions include:

- Discrimination has been further defined and “personal characteristics” (prohibited grounds) has been added as a definition instead of being part of the discrimination definition. “Indigenous Identity” has been added as a personal characteristic to align with its addition to the Human Rights Code.
- Harassment has been amended to provide clarity around what are “discriminatory harassment”, “sexual harassment”, and “bullying”; all of which continue to remain prohibited conduct.
- Definitions of terms not previously defined but referred to in the policy or procedure have been added for clarity.

In addition to a student advocate or union/employee representative, an individual can request that a support person (such as an Elder, friend, or family member) attend meetings with them and the RDI office.

The policy stresses the importance of confidentiality while the revisions provide additional clarity around confidentiality and when information can be disclosed by BCIT or RDI.

Under the current procedures, concerns regarding bullying, harassment, and discrimination can be addressed both informally or through a formal complaint process (through the RDI office or elsewhere), including an investigation. While the same options are still available, the revisions provide a clearer and more detailed explanation as to the various options an individual has to address a concern, and the roles and responsibilities of involved parties. Specifically, the revisions improve clarity or details about:

- who (in terms of positions, not individuals) concerns can be reported to;
- how the RDI office can assist when concerns are raised including through an informal voluntary resolution process;
- when and how an individual can file a formal complaint through the RDI Office and RDI's role in reviewing and accepting the complaint;
- options if a party to a complaint believes RDI to be in a conflict of interest;
- the opportunity for a voluntary resolution after a complaint has been filed with RDI and what occurs if a resolution is reached;
- what an investigation of a formal complaint by RDI involves, including what information will be contained in the resulting investigation report; and,
- what occurs if the policy is found to have been breached.

SUMMARY:

While much of the content has been changed for clarity, the revisions preserve the spirit and intent of the current policy and procedure. Further, the proposed revisions support the Institute's strategic plan including the core values of *championing diversity and inclusion* and *engaging with respect*, as well as its commitment to Indigenization and Reconciliation.

PREVENTION OF DISCRIMINATION, HARASSMENT, AND BULLYING – POLICY #7507

REVISED DRAFT

BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

Prevention of Discrimination, Harassment, and Bullying [DRAFT]

Policy No:	7507
Version:	6
Category:	
Approval Body:	Board of Governors
Executive Sponsor:	VP People, Culture, & Inclusion
Department Responsible:	People, Culture, & Inclusion (Respect, Diversity, & Inclusion Office)
Directory of Records Class:	0650-10
Approval Date:	YYYY MMM DD [tbd]

Policy Statement

This Policy (7507) and the related Procedure (7507-PR-1) were developed in consultation with, the British Columbia General Employees' Union (BCGEU) Support Bargaining Unit, BCGEU Faculty Bargaining Unit, the BCIT Faculty and Staff Association (BCITFSA), and the BCIT Student Association (BCITSA).

The British Columbia Institute of Technology (BCIT) recognizes that the BCIT community comprises individuals from many backgrounds, abilities, experiences, and identities, each contributing uniquely to the richness and diversity of the BCIT community as a whole. In recognition of this, BCIT fosters a climate of collaboration, understanding, and mutual respect between all members of the community. To that end BCIT and the above-mentioned parties:

- acknowledge that BCIT's main campuses are located on unceded Indigenous land belonging to the Coast Salish peoples, including the territories of the xʷməθkʷəy̓əm (Musqueam), Sḵwx̱wú7mesh (Squamish) Nations;
- are committed to providing a respectful, diverse, and inclusive learning and working environment free of Discrimination, Harassment, and Bullying (including retaliation as defined in this policy);
- champion diversity of experiences, ideas, cultures, and perspectives in a community of equity and inclusivity;
- expect all members of the BCIT community to contribute to a learning and working environment where the individuality of all students and employees is valued and respected; and,
- consider Discrimination, Harassment, and Bullying to be serious matters that undermine human dignity.

Purpose of Policy

The purpose of this Policy is to:

- communicate the importance of a respectful and inclusive learning and working environment, free of Discrimination, Harassment, and Bullying;
- define prohibited conduct;
- define the roles, rights, and responsibilities of all BCIT community members; and,
- establish education and prevention programs, and practices that support a respectful learning and working environment.

Table of Contents

Who This Policy Applies To

This Policy applies to all BCIT students, employees, contractors, volunteers, visitors, and members of the Board of Governors, during all BCIT-related activities.

Scope

BCIT-related activity includes any type of activity or communication directly related to or arising out of the operations of BCIT regardless of the location, including but not limited to: online and electronic communications; engagement with the public; practicums; field schools; co-ops; conferences; BCIT-sponsored events; participation in student clubs, teams, and social events sponsored by the Student Association or its clubs.

Related Documents and Legislation

Provincial Legislation

Apology Act, SBC 2006 c 19

College and Institute Act, RSBC 1996, c 52

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165

Human Rights Code, RSBC 1996, c 210

Labour Relations Code, RSBC 1996, c. 244

Sexual Violence and Misconduct Policy Act, SBC 2016, c 23

Workers Compensation Act, RSBC 2019, c 1

BCIT Policies

1000, Policy Development and Maintenance

1500, Code of Conduct

4501, Accommodation for Students with Disabilities

5102, Student Code of Conduct (Non-Academic)

6700, Freedom of Information and Protection of Privacy

7100, Safety and Security

7100-PR1, Response to Abusive or Threatening Behaviour Procedure

7103, Sexualized Violence

7150, Occupational Health and Safety

7511, Employment and Educational Equity

Definitions

The following definitions apply to this policy and its associated procedures:

"Complainant" means an individual who has filed a Formal Complaint under this Policy.

"Discrimination" refers to conduct - intentional or unintentional, individual or systemic – that:

- lacks bona fide justification and has the purpose or effect of causing an adverse impact (i.e., denial of an opportunity or imposition of a burden) to an individual or group on the basis of a Personal Characteristic (defined below); or,
- fails to provide reasonable accommodation (to the point of "undue hardship") for needs related to a Personal Characteristic.

It is not discrimination or a contravention of this Policy to implement an employment equity or other program or activity that has as its objective the amelioration of conditions of disadvantaged individuals or groups.

"Formal Complaint" means a written or otherwise documented statement provided in the manner required by the Procedure, alleging this Policy has been violated.

"Formal Resolution" means a voluntary agreement between parties to address concerns raised in a Formal Complaint filed under this Policy.

"Harassment" refers to conduct which meets any of the following definitions:

Discriminatory Harassment

Unwelcome, abusive, or demeaning behaviour, remarks, conduct or communications directed towards another person or persons that:

- include a direct or indirect reference to a Personal Characteristic; and,
- would be viewed by a reasonable person experiencing the behaviour as interfering with their participation in a BCIT-related activity, or, creating an intimidating, humiliating, or hostile environment.

Sexual Harassment

Unwelcome behaviour, remarks, conduct or communications of a sexual nature or due to a person's sex or gender, by a person:

- who knows or ought reasonably to know that the behaviour is unwanted or unwelcome; and,
- which interferes with another person's participation in a BCIT-related activity; or,
- leads to or implies job- or academically-related consequences for the person harassed.

Bullying and Harassment

Any inappropriate conduct or comment by one person towards another that the person knew or reasonably ought to have known would cause the other person to be humiliated or intimidated; excluding reasonable actions by an employer, supervisor, faculty member, or other person relating to the management, direction, training, education, or evaluation of others.

Harassment can occur during one incident, or over a series of incidents that individually would not necessarily constitute harassment.

"Informal Resolution" means a voluntary agreement between parties to address concerns related to conduct under this Policy where no Formal Complaint has been filed.

"Investigation" means a systematic inquiry into a Formal Complaint, conducted in accordance with the Procedure, to determine whether this Policy has been contravened.

"Personal Characteristics" means the following characteristics as well as any others specified in the BC *Human Rights Code* as grounds of discrimination ("prohibited grounds"):

Race, colour, ancestry, Indigenous identity, place of origin, political belief (in employment), religion, marital status, family status, physical disability or mental

disability, sex, gender identity, gender expression, sexual orientation, age, criminal or summary conviction unrelated to employment (in employment).

"Respondent" means an individual named in a Formal Complaint as having allegedly breached this Policy.

"Retaliation" means any adverse or threatened action, direct or indirect, taken by an individual against another individual for:

- invoking this Policy in good faith; or,
- participating or cooperating in any Formal or Informal Resolution or Investigation or in any other process pursuant to this Policy.

Retaliation is considered bullying and harassment and thus prohibited under this Policy and Procedure.

Duties and Responsibilities

BCIT

BCIT is responsible for providing a respectful learning and working environment by:

- preventing and discouraging Discrimination, Harassment, and Bullying, including through the delivery of education and awareness programs making students and employees aware of prohibited conduct under this Policy, and of the harms of Discrimination, Harassment, and Bullying and how to address them;
- providing an internal complaint process to address concerns of Discrimination, Harassment, and Bullying; and,
- ensuring appropriate outcomes and corrective actions where a Formal Complaint under this Policy is substantiated.

Members of the BCIT Community

Every member of the BCIT Community is:

- responsible for not engaging in Discrimination, Harassment, and Bullying, or any conduct contrary to this Policy;
- expected to adhere to all provisions set out in this Policy and Procedure including cooperating with any prescribed processes;
- strongly encouraged to promptly report suspected or alleged violations of this Policy;
- required to maintain confidentiality in accordance with this Policy;
- encouraged to engage with the Respect, Diversity and Inclusion Office ("RDI") at BCIT when addressing a concern or complaint.

The Steering Committee

The *Prevention of Discrimination, Harassment, and Bullying Steering Committee* (Steering Committee) comprises five members, with one representative from each of the following: BCIT; the BCGEU Support Bargaining Unit; the BCGEU Faculty Bargaining Unit; the BCITFSA; BCITSA.

The Steering Committee is responsible for:

- any revisions to this Policy and Procedure in accordance with the applicable Collective Agreements and BCIT Policy 1000;
- providing interpretations of this Policy and seeking external advice as needed to fulfill its responsibilities under the Policy;
- meeting at least twice annually or more often at the request of members;
- acting as the selection committee for RDI Advisors with the addition of the Head of RDI as a member of the selection committee;
- acting as the selection committee for the position of Head of RDI, with the addition of an RDI Advisor as a member of the selection committee;
- striving to reach consensus in any hiring decisions; and,
- creating and abiding by committee terms of reference.

The Respect, Diversity, and Inclusion Office (RDI)

RDI is responsible for:

- coordinating the development and delivery of appropriate education and awareness for employees and students related to the prevention of Discrimination, Harassment, and Bullying;
- providing confidential advisory services to any member of the BCIT community regarding any issues related to this Policy;
- facilitating the voluntary resolution of informal concerns and Formal Complaints under this Policy and Procedure;
- Administering the Investigation of Formal Complaints under this Policy and Procedure;
- acting as a resource to the Steering Committee; and,
- taking any other actions deemed appropriate by RDI to contribute to a respectful, diverse, and inclusive learning and working environment.

Consequences of Policy Violation

Any breach of this Policy may result in discipline up to and including termination of employment (for employees) or expulsion (for students).

Contractors, visitors to BCIT, and other third parties are expected to comply with this Policy. BCIT shall take reasonable action to address concerns related to conduct prohibited under this Policy, including denying or revoking access to BCIT property or events.

Other Information

1. Frivolous and Vexatious Complaints

Any person who makes a frivolous or vexatious complaint may be subject to disciplinary action. Frivolous or vexatious complaints may themselves be grounds for a complaint of Bullying and Harassment. Any complaint that is found to be frivolous, vexatious, malicious, or made in bad faith will constitute Bullying and Harassment under this Policy.

2. Time Limit

Anyone who believes this Policy may have been contravened is encouraged to raise their concern as soon as possible. For a Complaint to be accepted under this Policy, it should be filed within one year of the last incident of prohibited conduct. The Head of RDI may waive this time limit where extenuating circumstances prevented the Complainant from filing the Complaint in time. When considering whether to grant an extension, prejudice to the Respondent(s) will be considered, in addition to other factors.

If the request to file a Complaint beyond the one-year time limit is denied the Head of RDI will provide reasons for the denial, which may be appealed to the Board of Inquiry.

3. Multiple Proceedings

External Proceedings

Filing a Complaint under this Policy and Procedure does not preclude an individual from pursuing a complaint with the Human Rights Tribunal, WorkSafe BC, or other non-BCIT authority.

Internal Proceedings at BCIT

A Complainant may not initiate multiple proceedings at BCIT to deal with the same issue. The Head of RDI may decline to accept or may not proceed with all or part of a Complaint where it is fairly and adequately addressed by another BCIT proceeding, including but not limited to a grievance under a collective agreement, internal governance process of any party to this Policy, or proceeding under BCIT's Student Code of Conduct (Non-Academic).

4. Representation

In all meetings or discussions with RDI, or other meetings or hearings in relation to an informal concern or Formal Complaint under this Policy and Procedure:

- Employees who are members of a bargaining unit have a right to have union representation present at all stages of the process. Representation shall be afforded to employee members in accordance with the policies and practices of the union.

- RDI will permit students involved to request and obtain representation by the BCIT Student Association. Representation shall be afforded in accordance with the polices and practices of the Student Association.
- Where a current or former excluded employee is involved, RDI will permit that individual to obtain representation by another BCIT excluded employee of their choosing.

5. Support Person

In meetings or discussions with RDI, or other meetings or hearings in relation to an informal concern or Formal Complaint under this Policy and Procedure, an individual may request that a "support person" attend. Permission to allow a support person to attend will not be unreasonably withheld by RDI.

A support person can include but is not limited to a union representative, Elder, counsellor, friend, or family member. The role of a support person is not to represent or to speak for the person. Rather, they may attend meetings to observe and provide emotional support. The support person should be someone who is not involved in the concern or complaint being discussed and who would not be expected to be a witness should the matter proceed to an investigation. The support person is bound by confidentiality.

6. Procedural Fairness

The principles of procedural fairness shall be adhered to by all involved in the processes set out to deal with Discrimination, Harassment, or Bullying. All parties to the Discrimination, Harassment, or Bullying Complaint, including Complainants, Respondents, and witnesses, will be given the opportunity to fully explain what happened from their perspective, to have their explanations, evidence, and concerns fully and impartially considered, and to challenge any evidence being considered.

7. Cost Sharing

All costs arising in filing Formal Complaints with RDI shall be borne by BCIT.

Where the parties proceed to a Board of Inquiry, costs shall be shared by BCIT, the BCIT Faculty and Staff Association, the BCGEU Support Bargaining Unit, and the BCGEU Faculty Bargaining Unit as follows:

- BCIT always pays one-third of the total cost;
- BCIT also pays one-third of the total cost for each Complainant or Respondent who is either a management or excluded employee or a student;
- The bargaining unit shall pay one-third of the total cost for each Complainant or Respondent who is their member

Confidentiality

Personal information

In accordance with its obligations under *the Freedom of Information and Protection of Privacy Act* ("FIPPA") and Policy 6700*,* Freedom of Information and Protection of Privacy, BCIT will protect the privacy and confidentiality of staff, students, and other individuals involved in matters covered by this Policy. Personal information collected under this Policy will only be used and disclosed by BCIT as permitted or required under FIPPA and will be shared internally strictly on a need-to-know basis.

Complaints

Complaints filed under the Policy and addressed under the Procedures may involve the collection, use, and disclosure of sensitive personal information. Confidentiality is required so that those who may have experienced Discrimination, Harassment, or Bullying feel free to report it. It is also required for the protection of the reputations and interests of those accused of Discrimination, Harassment, or Bullying. However, any party may discuss the case in confidence with their supervisor, support person, or representative.

Subject to any limits or disclosure requirements imposed by law or by this Policy and Procedure, all information created, discovered, and collected through a Complaint in any form is to be treated as confidential by the Respondent and Complainant, their representatives, support persons, witnesses, and those administering the Policy.

Requests for RDI advice or information

Requests to RDI for advice or information related to matters under this Policy will be held in confidence, and RDI will limit access to Complaint files and related information and maintain them securely. Such information and documentation will only be released or disclosed by BCIT or by RDI on a need-to-know basis and as permitted by FIPPA or required by law, including:

- to address the emotional, psychological, or physical safety of any individual;
- to implement interim steps pending the outcome of an Investigation;
- to resolve and implement a voluntary Resolution;
- to conduct an Investigation;
- after a formal finding that the Policy has been breached.

Procedures Associated with This Policy

Prevention of Discrimination, Harassment, and Bullying Procedure – PR1

Forms Associated with This Policy

None

Amendment History

	Approval Date	Status
Created: 7507, Harassment & Discrimination version 1	1993 Nov 23	Replaced
Revised: 7507, Harassment & Discrimination version 2	2002 Jan 31	Replaced
Revised: 7507, Harassment & Discrimination version 3	2009 May 03	Replaced
Revised: 7507, Harassment & Discrimination version 4	2010 June 29	Replaced
Revised: 7507, Harassment & Discrimination version 5	2014 July 22	In Force
Revised: 7507, Prevention of Discrimination, Harassment & Bullying version 6 [draft]	tbd	In review

Scheduled Review Date

This Policy 7507 and Procedure 7507-PR1 are ratified by BCIT, the BCGEU Support Bargaining Unit, BCGEU Faculty Bargaining Unit, the BCIT Faculty and Staff Association, and the BCIT Student Association.

TBD - approval date + 5 years [yyyy mmm dd]; or earlier if regulatory or operational changes require it. By mutual agreement, the parties may at any time develop and propose amendments to the Policy or the Procedures for review and approval by the Board of Governors.

PREVENTION OF DISCRIMINATION, HARASSMENT, AND BULLYING – POLICY #7507

REDLINE

Prevention of Discrimination, Harassment, and Bullying ~~Harassment and Discrimination~~

Policy No.:	7507
Version:	6
Category:	~~Administration~~
Approving Body:	Board of Governors ~~Leadership Team~~
Executive Sponsor~~Division:~~	VP People, Culture, & Inclusion ~~President~~
Department Responsible:	People, Culture, & Inclusion (Respect, Diversity, & Inclusion Office) ~~Harassment and Discrimination Advisor~~
Directory of Records Class:	0650-10
~~Current~~ Approval~~ed~~ Date:	[tbd]~~2014 Jul 22~~

Policy Statement

This Policy (7507) and the related Procedure (7507-PR-1) were developed in consultation with, the British Columbia General Employees' Union (BCGEU) Support Bargaining Unit, BCGEU Faculty Bargaining Unit, the BCIT Faculty and Staff Association (BCITFSA), and the BCIT Student Association (BCITSA).

The British Columbia Institute of Technology (BCIT) recognizes that the BCIT community comprises individuals from many backgrounds, abilities, experiences, and identities, each contributing uniquely to the richness and diversity of the BCIT community as a whole. In recognition of this, BCIT fosters a climate of collaboration, understanding, and mutual respect between all members of the community. To that end BCIT and the above-mentioned parties:

~~The British Columbia Institute of Technology, the British Columbia Government and Services Employees' Union (BCGEU) Local 703 Support and Instructional Bargaining Units, the BCIT Faculty and Staff Association and the Student Association agree that all members of the BCIT community are entitled to work and learn in an environment free from Bullying and Harassment and Discrimination. To that end, these parties:~~

- acknowledge that BCIT's main campuses are located on unceded Indigenous land belonging to the Coast Salish peoples, including the territories of the xʷməθkʷəy̓əm (Musqueam), Sḵwx̱wú7mesh (Squamish) Nations;
- ~~A~~are committed to providing a respectful, diverse, and inclusive learning and working environment free of Discrimination, Harassment, and Bullying (including retaliation as defined in this policy) ~~where the individual differences of all students and employees are valued and respected.~~
- ~~Will not condone and will not tolerate any Discrimination, Bullying or Harassing behaviour which undermines the dignity, self-esteem, and productivity of any student or employee.~~champion diversity of experiences, ideas, cultures, and perspectives in a community of equity and inclusivity;
- expect all members of the BCIT community to contribute to a learning and working environment where the individuality of all students and employees is valued and respected; and
- ~~C~~consider Discrimination, Harassment, and Bullying ~~Bullying and Harassment and/or Discrimination by any employee or student~~ to be a serious matters that undermine human dignity~~breach of human rights which requires immediate resolution. Such resolution may include disciplinary measures up to and including dismissal or expulsion~~.

~~All members of the BCIT community are expected to promote a learning and working environment of mutual trust and respect. Nothing in this policy or its associated Procedure 7507-PR1, Harassment and~~

~~Discrimination derogates from the responsibility or the role of managers of BCIT to ensure a work and educational environment that is free from Bullying and Harassment and Discrimination. BCIT is responsible to prevent and remedy situations of Bullying and Harassment and/or Discrimination as they occur.~~

Purpose of Policy

The purpose of this Policy is to:

- communicate the importance of a respectful and inclusive learning and working environment, free of Discrimination, Harassment, and Bullying;
- define prohibited conduct;
- define the roles, rights, and responsibilities of all BCIT community members; and,
- establish education and prevention programs, and practices that support a respectful learning and working environment.

Table of Contents

[…]

Who This Policy Applies To~~Application of this Policy~~

This policy applies to all BCIT students, employees, contractors, ~~of BCIT, and contract employees~~ and members of the Board of Governors, during all BCIT-related activities.

Related Documents and Legislation

Provincial Legislation

Apology Act, SBC 2006 c 19
Colleges and Institute~~s~~ Act, RSBC 1996, c.52
Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165
~~British Columbia~~ Human Rights Code, RSBC 1996, c.210
Labour Relations Code, RSBC 1996, c. 244
Sexual Violence and Misconduct Policy Act, SBC 2016, c 23
Workers Compensation Act, RSBC 2019~~1996~~, c 1~~.492~~
~~Labour Relations Code, RSBC 1996, c. 244~~

BCIT Policies

1000, Policy Development and Maintenance
1500, Code of Conduct
4501, Accommodation for Students with Disabilities
5102, Student Code of Conduct (Non-Academic)
6700, Freedom of Information and Protection of Privacy
7100, Safety and Security
7100-PR1, Response to Abusive or Threatening Behaviour Procedure
7103, Sexualized Violence
7150, Occupational Health and Safety
7511, Employment and Educational Equity

Definitions

The following definitions apply to this policy and its associated procedures:

***"Complainant"** means an individual who has filed a Formal Complaint under this Policy.*

~~**BCIT Community**~~

~~The BCIT community includes all BCIT students, employees and contract employees.~~

~~**Discrimination**~~
~~Discrimination, as it applies to BCIT's students, is defined as denial of any accommodation, service, facility, or opportunity that is customarily available to the public, because of the race, color, ancestry, place of origin, religion, marital status, family status, physical or mental disability, gender, or sexual orientation of the individual who was denied the accommodation, service, facility, or opportunity, except where there is a bona fide educational requirement.~~

~~Discrimination, as it applies to BCIT's employees, is defined as refusing to employ or to continue to employ a person, or refusing to provide an opportunity or benefit with respect to employment or any term or condition of employment, because of the race, color, ancestry, place of origin, political belief, religion, marital status, family status, sexual orientation, physical or mental disability, gender, or unrelated criminal or summary conviction of that person, except where there is a bona fide occupational requirement.~~

"Discrimination" refers to conduct - intentional or unintentional, individual or systemic – that:

• lacks bona fide justification and has the purpose or effect of causing an adverse impact (i.e., denial of an opportunity or imposition of a burden) to an individual or group on the basis of a Personal Characteristic (defined below); or,
• fails to provide reasonable accommodation (to the point of "undue hardship") for needs related to a Personal Characteristic.

It is not discrimination or a contravention of this Policy to implement an employment equity or other program or activity that has as its objective the amelioration of conditions of disadvantaged individuals or groups.

"Formal Complaint" means a written or otherwise documented statement provided in the manner required by the Procedure, alleging this Policy has been violated.

"Formal Resolution" means a voluntary agreement between parties to address concerns raised in a Formal Complaint filed under this Policy.

~~**Harassment**~~
~~Harassment, for the purposes of this policy, is defined as any unwelcome remarks, behaviours or communications based on race, colour, ancestry, place of origin, political belief, religion, marital status, family status, sexual orientation, physical or mental disability, gender, age, or criminal or summary conviction which causes offense or humiliation to any person, and:~~

- ~~Submission to such conduct becomes explicitly or implicitly a term or condition of employment or the learning environment; or~~
- ~~Submission to or rejection of such conduct is used as a basis for employment or educational decisions; or~~
- ~~Such conduct has the purpose or effect of interfering with work or educational performance; or~~
- ~~Such conduct creates an intimidating, hostile, or offensive working or educational environment.~~

"Harassment" refers to conduct which meets any of the following definitions:

Discriminatory Harassment

Unwelcome, abusive, or demeaning behaviour, remarks, conduct or communications directed towards another person or persons that:

• include a direct or indirect reference to a Personal Characteristic; and,
• would be viewed by a reasonable person experiencing the behaviour as interfering with their participation in a BCIT-related activity, or, creating an intimidating, humiliating, or hostile environment.

Sexual Harassment

Unwelcome behaviour, remarks, conduct or communications of a sexual nature or due to a person's sex or gender, by a person:

- who knows or ought reasonably to know that the behaviour is unwanted or unwelcome; and,
- which interferes with another person's participation in a BCIT-related activity; or,
- leads to or implies job- or academically-related consequences for the person harassed.

~~**Sexual Harassment**~~
~~Sexual Harassment is unwelcome sexually oriented conduct, which may be either verbal, physical, or by innuendo, where:~~

- ~~Submission to such conduct is made either explicitly or implicitly a term or condition of employment or of educational progress; or~~
- ~~Submission to or rejection of such conduct is used as a basis for employment or educational decisions; or~~
- ~~Such conduct has the purpose or effect of interfering with work or educational performance; or~~
- ~~Such conduct creates an intimidating, hostile, or offensive working or educational environment.~~

~~**Personal Harassment**~~
~~Personal Harassment is defined as unwelcome remarks, behaviours or communications directed toward an individual or a group of individuals which misuses authority, or abuses the power one individual or a group of individuals has over an individual or a group of individuals. For the purposes of this Policy, the term power is intended to mean more than the power that is vested in an individual or position by the Institute. Power in this context includes any type of power that one individual may have over another individual. Misuse or abuse of power occurs when it has the effect or purpose of seriously abusing, threatening, demeaning, or intimidating the individual or group of individuals, and:~~

- ~~Submission to such conduct is made either explicitly or implicitly a term or condition of employment or of educational progress; or~~
- ~~Submission to or rejection of such conduct is used as a basis for employment or educational decisions; or~~
- ~~Such conduct has the purpose or effect of interfering with work or educational performance; or~~
- ~~Such conduct creates an intimidating, hostile, or offensive working or educational environment.~~

Bullying and Harassment

Any inappropriate conduct or comment by one person towards another that the person knew or reasonably ought to have known would cause the other person to be humiliated or intimidated; excluding reasonable actions by an employer, supervisor, faculty member, or other person relating to the management, direction, training, education, or evaluation of others.

Harassment can occur during one incident, or over a series of incidents that individually would not necessarily constitute harassment.

~~**Bullying and Harassment**~~
~~Bullying and Harassment per WorkSafe BC means:~~

- ~~Includes any inappropriate conduct or comment by a person towards a worker that the person knew or reasonably ought to have known would cause that worker to be humiliated or intimidated, but~~
- ~~Excludes any reasonable action taken by an employer or supervisor relating to the management and direction of workers or the place of employment.~~

~~Examples of conduct or comments that might constitute bullying and harassment include verbal aggression or insults, calling someone derogatory names, harmful hazing or initiation practices, vandalizing personal~~

~~belongings, and spreading malicious rumours.~~

"Informal Resolution" means a voluntary agreement between parties to address concerns related to conduct under this Policy where no Formal Complaint has been filed.

"Investigation" means a systematic inquiry into a Formal Complaint, conducted in accordance with the Procedure, to determine whether this Policy has been contravened.

"Personal Characteristics" means the following characteristics as well as any others specified in the BC Human Rights Code as grounds of discrimination ("prohibited grounds"):

> Race, colour, ancestry, Indigenous identity, place of origin, political belief (in employment), religion, marital status, family status, physical disability or mental disability, sex, gender identity, gender expression, sexual orientation, age, criminal or summary conviction unrelated to employment (in employment).

"Respondent" means an individual named in a Formal Complaint as having allegedly breached this Policy

"**Retaliation**" means any adverse or threatened action, direct or indirect, taken by an individual against another induvial for;

- Invoking this Policy in good faith; or,
- Participating or cooperating in any Formal or Informal Resolution or Investigation or in any other process pursuant to this Policy.

Retaliation ~~against any individual who has filed a complaint, or who has been named as a Respondent or witness in the complaint or who investigates the complaint according to Procedure 7507-PR1 shall itself be an incident of~~ is considered bullying and harassment and thus prohibited under this Policy and Procedure. ~~may result in disciplinary action.~~

~~Other Information~~

~~It is recognized that Bullying and Harassing or Discriminatory behaviour, as defined in this Policy, may be unintentional and that those responsible may not be aware of the offense they are causing and the effect their behaviour may have on the work or educational environment.~~
~~Discrimination, Bullying and Harassment can occur between individuals of the same or different status and both men and women can be the subject of Bullying and Harassment by members of either gender.~~

~~Discrimination, Bullying and Harassment can involve individuals or groups; can occur during one incident, or over a series of incidents, which, in isolation, would not necessarily constitute Bullying and Harassment; and can occur on campus or off, during working hours or not.~~

Duties and~~,~~ Responsibilities~~, and General Information~~

~~1. Education and Prevention~~

~~A crucial component of this policy is the provision for education about Bullying and Harassment and Discrimination which will encourage awareness and prevention. BCIT will endeavour to ensure that all employees and students are made aware of what constitutes Bullying and Harassment and Discrimination, why it is so harmful to those who are hurt or offended by it and what individuals can do to take corrective action. The BCGEU Local 703 Support and Instructional Bargaining Units, the BCIT Faculty and Staff Association, and the Student Association as parties to this agreement support and encourage BCIT's endeavours.~~

BCIT

BCIT is responsible for providing a respectful learning and working environment by:

• preventing and discouraging Discrimination, Harassment, and Bullying, including through the delivery of education and awareness programs making students and employees aware of prohibited conduct under this Policy, and of the harms of Discrimination, Harassment, and Bullying and how to address them;
• providing an internal complaint process to address concerns of Discrimination, Harassment, and Bullying; and,
• ensuring appropriate outcomes and corrective actions where a Formal Complaint under this Policy is substantiated.

Members of the BCIT Community

Every member of the BCIT Community is:

• responsible for not engaging in Discrimination, Harassment, and Bullying, or any conduct contrary to this Policy;
• expected to adhere to all provisions set out in this Policy and Procedure including cooperating with any prescribed processes;
• strongly encouraged to promptly report suspected or alleged violations of this Policy;
• required to maintain confidentiality in accordance with this Policy;
• encouraged to engage with the Respect, Diversity and Inclusion Office ("RDI") at BCIT when addressing a concern or complaint.

The Steering Committee

The *Prevention of Discrimination, Harassment, and Bullying Steering Committee* (Steering Committee) comprises five members, with one representative from each of the following: BCIT; the BCGEU Support Bargaining Unit; the BCGEU Faculty Bargaining Unit; the BCITFSA; BCITSA.

The Steering Committee is responsible for:

• any revisions to this Policy and Procedure in accordance with the applicable Collective Agreements and BCIT Policy 1000;
• providing interpretations of this Policy and seeking external advice as needed to fulfill its responsibilities under the Policy;
• meeting at least twice annually or more often at the request of members;
• acting as the selection committee for RDI Advisors with the addition of the Head of RDI as a member of the selection committee;
• acting as the selection committee for the position of Head of RDI, with the addition of an RDI Advisor as a member of the selection committee;
• striving to reach consensus in any hiring decisions; and,
• creating and abiding by committee terms of reference.

~~13.~~ **Steering Committee**

~~There shall be a steering committee comprising members representing the parties to this policy. The steering committee shall provide interpretation of this policy and shall be responsible for any revisions to the Policy and Procedure 7507-PR1. The committee shall meet at least quarterly and more often if requested by members of the committee. The Advisor shall be a resource to the steering committee.~~

~~2. The Harassment and Discrimination Advisor~~

~~BCIT, in consultation with the Harassment and Discrimination Steering Committee, will act as a selection committee for the position of Harassment and Discrimination Advisor (Advisor). The Advisor will carry out the roles as set out in this Policy and Procedure 7507-PR1.~~

~~The role of the Advisor is to provide prevention-oriented education and confidential advisory services to the BCIT community, which promotes understanding and awareness of Bullying and Harassment and Discrimination issues.~~
~~Specifically the Advisor shall:~~
~~• Act as a resource for all members of the BCIT Community who require general or specific~~

~~information on Bullying and Harassment or Discrimination.~~

- ~~Be available to provide confidential advice or information about Bullying and Harassment or Discrimination issues to any student, employee, or contract employee.~~
- ~~Coordinate the development and delivery of appropriate training and education to employees and students on Bullying and Harassment and Discrimination issues according to this Policy and Procedure 7507-PR1.~~
- ~~Facilitate the resolution of complaints filed under this policy, and assist members of the BCIT community to effectively resolve interpersonal conflicts where Bullying and Harassment or Discrimination may be an issue.~~

The Respect, Diversity, and Inclusion Office (RDI)

RDI is responsible for:

• coordinating the development and delivery of appropriate education and awareness for employees and students related to the prevention of Discrimination, Harassment, and Bullying;
• providing confidential advisory services to any member of the BCIT community regarding any issues related to this Policy;
• facilitating the voluntary resolution of informal concerns and Formal Complaints under this Policy and Procedure;
• Administering the Investigation of Formal Complaints under this Policy and Procedure;
• acting as a resource to the Steering Committee; and,
• taking any other actions deemed appropriate by RDI to contribute to a respectful, diverse, and inclusive learning and working environment.

Consequences of Policy Violation

Any breach of this Policy may result in discipline up to and including termination of employment (for employees) or expulsion (for students).

Contractors, visitors to BCIT, and other third parties are expected to comply with this Policy. BCIT shall take reasonable action to address concerns related to conduct prohibited under this Policy, including denying or revoking access to BCIT property or events.

Other Information

1. Frivolous and Vexatious Complaints

Any person who makes a frivolous or vexatious complaint may~~shall~~ be subject to disciplinary action. Frivolous or vexatious complaints may themselves be grounds for a complaint of Bullying and H~~h~~arassment. Any complaint that is found to be frivolous, vexatious, malicious, or made in bad faith will constitute Bullying and Harassment under this Policy.

2. ~~3.~~ Time Limit

Anyone who believes this Policy may have been contravened is encouraged to raise their concern as soon as possible. For a complaint to be accepted ~~considered~~ under this policy, it should~~must~~ be filed within one year of the last incident of prohibited conduct~~Bullying and Harassment or Discrimination~~. The Head of RDI ~~Advisor has the discretion to~~may waive this time limit ~~requirement~~ where there are extenuating circumstances which prevented the Complainant from filing the Complaint in time ~~complaint from being brought forward in that time frame. Participation in a successful or unsuccessful resolution attempt will constitute an extenuating circumstance for the purpose of this paragraph.~~ When considering whether to grant an extension, prejudice to the Respondents(s) will be considered, in addition to other factors.

If the request to file a Complaint beyond the one-year time limit is denied the Head of RDI will provide reasons for the denial, which may be appealed to the Board of Inquiry.

~~**4. Confidentiality**~~

~~Requests to the Advisor for advice or information will be held in strict confidence.~~

~~The name of the person filing the complaint (the Complainant), the person responding to the complaint (the Respondent), and the circumstances of the complaint will not be disclosed to any person except where disclosure is necessary for the purpose of investigating and resolving the complaint, taking any related disciplinary measures, or as required by law.~~

~~The confidentiality of complaints of Bullying and Harassment or Discrimination shall be respected by all those who are privy to information or in possession of documentation pertaining to matters/incidents relating to a complaint. This shall include refraining from discussions or releasing information in any form, beyond that outlined in this Policy and Procedure 7507-PR1 or as required by law.~~

~~Confidentiality is not the same as anonymity. The identity of the Complainant or Respondent may be disclosed by the Advisor if disclosure is necessary to facilitate the resolution of the complaint. The Complainant or Respondent will be advised if their identity will be disclosed.~~

~~Concerns for an individual's health, safety, and security, or legal proceedings such as arbitration, or requirements under the *Criminal Code* may require BCIT to disclose information about a complaint to individuals who may not be involved directly in the application of the procedures. In such a case the information will be disclosed through the Advisor with the authority of the President.~~
~~No documentation of the Bullying and Harassment or Discrimination, including any materials resulting from an informal or formal resolution process, such as reports from the Advisor, the alternate Advisor, or Board of Inquiry will be placed on the Complainant's personnel file or student record.~~

~~In the event that the conclusion of an Advisor's review is that Bullying and Harassment or Discrimination did occur and where disciplinary action was taken, a letter indicating the disciplinary action taken is the only documentation that will appear on the Respondent's personnel file or student record.~~
~~Any documentation, files, or records which relate to a complaint under this policy will be maintained in a confidential manner by the Advisor.~~

3. Multiple Proceedings

External Proceedings

Filing a Complaint under this Policy and Procedure does not preclude an individual from pursuing a complaint with the Human Rights Tribunal, WorkSafe BC, or other non-BCIT authority.

Internal Proceedings at BCIT

A Complainant may not initiate multiple proceedings at BCIT to deal with the same issue. The Head of RDI may decline to accept or may not proceed with all or part of a Complaint where it is fairly and adequately addressed by another BCIT proceeding, including but not limited to a grievance under a collective agreement, internal governance process of any party to this Policy, or proceeding under BCIT's Student Code of Conduct (Non-Academic).

4. ~~5.~~ Representation

In all meetings or discussions with RDI, or other meetings or hearings in relation to an informal concern or Formal Complaint under this Policy and Procedure:

- Employees who are members of a bargaining unit have a right to have union representation present at all stages of the process. Representation shall be afforded to employee members in accordance with the policies and practices of the union.
- RDI will permit students involved to request and obtain representation by the BCIT Student Association.

Representation shall be afforded in accordance with the polices and practices of the Student Association.

- Where a current or former excluded employee is involved, RDI will permit that individual to obtain representation by another BCIT excluded employee of their choosing.

~~The Complainant and Respondent are entitled to be represented by a union representative, where they are a member of a bargaining unit, or by a representative of the Student Association, where they are a student, in all meetings with the Advisor, the alternate Advisor, or other meetings or hearings in relation to a complaint under this Policy and Procedure 7507-PR1. The type of representation available for the Complainant or the Respondent at the Board of Inquiry stage is determined by the representative of the Complainant or Respondent.~~

~~Where either the Complainant or Respondent is a member of excluded staff, they are entitled to a representative who is an employee of the Institute in all meetings with the Advisor, the alternate Advisor, or other meetings or hearings in relation to a complaint under this Policy and Procedure 7507-PR1.~~

5. Support Person

In meetings or discussions with RDI, or other meetings or hearings in relation to an informal concern or Formal Complaint under this Policy and Procedure, an individual may request that a "support person" attend. Permission to allow a support person to attend will not be unreasonably withheld by RDI.

A support person can include but is not limited to a union representative, Elder, counsellor, friend, or family member. The role of a support person is not to represent or to speak for the person. Rather, they may attend meetings to observe and provide emotional support. The support person should be someone who is not involved in the concern or complaint being discussed and who would not be expected to be a witness should the matter proceed to an investigation. The support person is bound by confidentiality.

6. ~~Natural Justice and~~ Procedural Fairness

The principles of procedural ~~natural justice and~~ fairness shall be adhered to by all involved in the processes ~~anyone who becomes involved in any aspect of the proce~~ss set out to deal with Discrimination, Harassment, or Bullying. ~~Bullying and Harassment or Discrimination. This means that a~~All parties to the ~~Bullying and Harassment or~~ Discrimination, Harassment, or Bullying complaint, including ~~the~~ Complainants, Respondents, and witnesses, will be given the opportunity to fully explain what happened from their perspective, to have their explanations, evidence, and concerns fully and impartially considered, and to challenge any evidence ~~that is~~ being ~~or has been~~ considered.

~~**7. Retaliation**~~

~~Retaliation against any individual who has filed a complaint, or who has been named as a Respondent or witness in the complaint or who investigates the complaint according to Procedure 7507-PR1 shall itself be an incident of harassment and may result in disciplinary action.~~

~~**8. Vexatious Complaints**~~
~~Any person who makes a frivolous or vexatious complaint shall be subject to disciplinary action. Frivolous or vexatious complaints may themselves be grounds for a complaint of harassment.~~

7. ~~9.~~ Cost Sharing

All costs arising in~~from~~ filing Formal Complaints with RDI ~~a complaint with the Advisor or from a review by an Alternate Advisor~~ shall be borne by BCIT.

Where the parties proceed to a Board of Inquiry, ~~the~~ costs ~~of the Board of Inquiry~~ shall be shared by BCIT, the BCIT Faculty and Staff Association, and the BCGEU Support Bargaining Unit, and the BCGEU Faculty Bargaining Unit as follows:

- BCIT always pays one-third of the total cost;
- BCIT also pays one-third of the total cost for each Complainant or Respondent who is either a management or excluded employee or a student;
- The bargaining unit shall pay one-third of the total cost for each Complainant or Respondent who is their member

- ~~Where the Complainant and Respondent are members of the same bargaining unit, BCIT shall pay 1/3 of the cost and the bargaining unit shall pay the other 2/3.~~
- ~~Where the Complainant and Respondent are not members of the same bargaining unit, BCIT shall pay 1/3 of the total cost and the bargaining units shall each pay 1/3 of the total cost.~~
- ~~Where either the Complainant and/or Respondent is a management or excluded employee, BCIT shall pay 1/3 of the total cost, plus 1/3 of the cost in respect of the Complainant and/or Respondent who is a management or excluded employee. Where either the Complainant or Respondent in this instance is a member of a bargaining unit, that bargaining unit shall pay the remaining 1/3 of the cost.~~
- ~~Where either the Complainant and/or Respondent is a student, BCIT shall pay 1/3 of the total cost, plus the cost in respect of the Complainant and/or Respondent who is a student.~~

~~10. British Columbia Human Rights Tribunal~~

~~Employees and students should also be aware that they may file a complaint of harassment or discrimination with the B.C. Human Rights Tribunal.~~

~~11. Grievance and Arbitration~~

~~BCIT, the BCGEU Local 703 Support and Instructional Bargaining Units, and the BCIT Faculty and Staff Association agree that the complaint and investigation processes provided in this policy constitute the grievance process for any and all complaints of Bullying and Harassment and Discrimination on grounds included in this policy and involving employees who are members of bargaining units.~~

~~In such cases employees shall not have access to the other grievance processes in the collective agreements.~~

~~The aforementioned parties further agree that the Board of Inquiry provided for in this policy is a Board of Arbitration as provided under the *Labour Relations Code* of British Columbia, which will render (when required) a final and binding determination in any and all complaints of Bullying and Harassment and Discrimination involving employees who are members of bargaining units.~~

~~12. Appeal to Board of Governors~~

~~A student who is disciplined pursuant to Section 37(2) of the *Colleges and Institutes Act*, RSBC 1996, c.52 under this policy retains a right to appeal that discipline to the Board of Governors. If a student elects to appeal discipline implemented under this policy to the Board of Governors, a decision by the Board of Governors regarding the discipline is final and determinative of the matter. As well, by electing to appeal to the Board of Governors, the student is precluded from pursuing a review by a Board of Inquiry on the matter of discipline.~~

~~An employee, who is suspended pursuant to Section 37(1) of the *Colleges and Institutes Act*, RSBC 1996, c.52 under this policy, retains a right to appeal that suspension to the Board of Governors. If the employee elects to appeal a suspension implemented as a form of discipline under this policy to the Board of Governors, a decision by the Board of Governors regarding the suspension is determinative of the matter. As well by electing to appeal to the Board of Governors, the member of the instructional, administrative and other staff is precluded from pursuing a review by a Board of Inquiry on the matter of the suspension~~

~~13. Steering Committee~~

~~There shall be a steering committee comprising members representing the parties to this policy. The steering committee shall provide interpretation of this policy and shall be responsible for any revisions to the Policy and Procedure 7507-PR1. The committee shall meet at least quarterly and more often if~~

~~requested by members of the committee. The Advisor shall be a resource to the steering committee.~~

Confidentiality

Personal information

In accordance with its obligations under the Freedom of Information and Protection of Privacy Act ("FIPPA") and Policy 6700, Freedom of Information and Protection of Privacy, BCIT will protect the privacy and confidentiality of staff, students, and other individuals involved in matters covered by this Policy. Personal information collected under this Policy will only be used and disclosed by BCIT as permitted or required under FIPPA and will be shared internally strictly on a need-to-know basis.

Complaints

Complaints filed under the Policy and addressed under the Procedures may involve the collection, use, and disclosure of sensitive personal information. Confidentiality is required so that those who may have experienced Discrimination, Harassment, or Bullying feel free to report it. It is also required for the protection of the reputations and interests of those accused of Discrimination, Harassment, or Bullying. However, any party may discuss the case in confidence with their supervisor, support person, or representative.

Subject to any limits or disclosure requirements imposed by law or by this Policy and Procedure, all information created, discovered, and collected through a Complaint in any form is to be treated as confidential by the Respondent and Complainant, their representatives, support persons, witnesses, and those administering the Policy.

Requests for RDI advice or information

Requests to RDI for advice or information related to matters under this Policy will be held in confidence, and RDI will limit access to Complaint files and related information and maintain them securely. Such information and documentation will only be released or disclosed by BCIT or by RDI on a need-to-know basis and as permitted by FIPPA or required by law, including:

- to address the emotional, psychological, or physical safety of any individual;
- to implement interim steps pending the outcome of an Investigation;
- to resolve and implement a voluntary Resolution;
- to conduct an Investigation;
- after a formal finding that the Policy has been breached.

Procedures Associated With This Policy

Prevention of Discrimination, Harassment, and Bullying Procedure – PR1
~~Procedure 7507-PR1, Harassment and Discrimination~~

~~14. Periodic Review of Policy and Procedures~~

~~This Policy 7507 and Procedure 7507-PR1 are ratified for a three year period by BCIT, the BCGEU Local 703 Support Staff and Instructional Bargaining Units, the BCIT Faculty and Staff Association, and the Student Association. During this time, amendments or revisions to the policy or the procedures may be made by mutual agreement of the parties. A formal review of the policy will be conducted annually. Any renewal or revision of this agreement must be mutually agreed to by all the parties to the agreement.~~

Forms Associated With This Policy

None
~~See procedure for list of forms.~~

Amendment History

	Approval Date	Status
Created: 7507, Harassment & Discrimination version 1	1993 Nov 23	Replaced
Revised: 7507, Harassment & Discrimination version 2	2002 Jan 31	Replaced
Revised: 7507, Harassment & Discrimination version 3 2	009 May 03	Replaced
Revised: 7507, Harassment & Discrimination version 4	2010 June 29	Replaced
Revised: 7507, Harassment & Discrimination version 5	2014 July 22	In Force
Revised: 7507, Prevention of Discrimination, Harassment & Bullying version 6 [draft] tbd		In review

~~Created 1993 Nov 23~~
~~Revision 1 2002 Jan 31~~
~~Revision 2 2010 Jun 29~~
~~Revision 3 2014 Jul 22~~

Scheduled Review Date

This Policy 7507 and Procedure 7507-PR1 are ratified by BCIT, the BCGEU~~for a three year period by BCIT, the BCGEU Local 703~~ Support ~~Staff and Instructional~~ Bargaining Units~~,~~ BCGEU Faculty Bargaining Unit, the BCIT Faculty and Staff Association, and the BCIT Student Association.

TBD -approval date + 5 years [yyy mmm dd]; or earlier if regulatory or operational changes require it. ~~During this time, amendments or revisions to the policy or the procedures may be made b~~By mutual agreement, ~~of~~ the parties~~. A formal review of the policy will be conducted annually.~~ may at any time develop and propose amendments to the Policy or the Procedures for review and approval by the Board of Governors.
~~Any renewal or revision of this agreement must be mutually agreed to by all the parties to the agreement.~~

~~2015 July~~

PREVENTION OF DISCRIMINATION, HARASSMENT, AND BULLYING – PROCEDURE #7507-PR1

REVISED DRAFT

BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

Prevention of Discrimination, Harassment, and Bullying [DRAFT]

Procedure No:	7507-PR1
Version:	4
Policy Reference:	7507, Prevention of Discrimination, Harassment, and Bullying
Category:	
Approval Body:	Board of Governors
Executive Sponsor:	
Department Responsible:	People, Culture, & Inclusion (Respect, Diversity, & Inclusion Office)
Directory of Records Class:	0650-10
Approval Date:	YYYY MMM DD [TBD]

Objectives

This Procedure forms part of Policy 7507, Prevention of Discrimination, Harassment, and Bullying. This Procedure provides a fair and equitable process for the resolution of concerns and Formal (written or otherwise documented) complaints of Discrimination, Harassment, or Bullying (including retaliation as defined in the Policy).

Who This Procedure Applies To

This Policy applies to all BCIT students, employees, contractors, volunteers, visitors, and members of the Board of Governors, during all BCIT-related activities.

Scope

BCIT-related activity includes any type of activity or communication directly related to or arising out of the operations of BCIT regardless of the location, including but not limited to: online and electronic communications; engagement with the public; practicums; field schools; co-ops; conferences; BCIT-sponsored events; participation in student clubs, teams, and social events sponsored by the Student Association or its clubs.

Purpose

The purposes of this Procedure are:

- to communicate how concerns relating to conduct prohibited under the Policy are to be addressed; and,
- to set out the roles, rights, and responsibilities of parties to a Complaint.

Related Documents and Legislation

As set out in the Policy.

Definitions

The terms and meanings in this Procedure are as used and defined in the Policy.

Table of Contents [TBD]

Duties and Responsibilities

Preventing and Responding to Concerns Relating to Discrimination, Harassment, or Bullying

All BCIT Community Members including employees and students

Individuals are encouraged to resolve concerns informally, if they feel safe doing so. An individual may directly advise a person they believe has behaved inappropriately that the behaviour is unwelcome.

Any individual who believes they have been or are being subjected to Discrimination, Harassment, or Bullying as defined in Policy 7507 should keep a record of the incident or incidents of the prohibited behaviour including dates, times, what happened, and names of any witnesses.

All *employees* are expected to report any behaviour that they believe could constitute Bullying and Harassment to a person in authority, even if they do not wish to make a Formal Complaint.

Members of the BCIT community are strongly encouraged to report any instances of suspected Discrimination, Harassment, or Bullying to a person in authority, especially if they or others have been unable to resolve it directly.

BCIT Employees with management or supervisory authority

BCIT personnel who manage or supervise employees have an obligation to take reasonable steps within their scope of authority to prevent and respond to Discrimination, Harassment, or Bullying they are aware of.

Faculty and Faculty Instructors responsible for students have an obligation to take reasonable steps within the scope of their authority to prevent and respond to Discrimination, Harassment, or Bullying of their students they are aware of.

All employees are encouraged to contact RDI with any questions about how to fulfill their responsibilities.

RDI

Anyone believing or suspecting that Policy 7507 may have been breached, whether or not they are the individual subjected to the conduct in question, can contact RDI for confidential advice and information.

RDI will listen to the concern raised, ask questions, and provide relevant information appropriate to the situation. Such advice or information may include an assessment of

whether the alleged behaviour appears to be conduct prohibited by the Policy, options for resolutions under this Procedure or other ways of addressing the concerns, and any referrals deemed appropriate.

RDI does not provide legal advice, nor does it advocate for any party.

Procedure

1. Reporting Concerns

Reporting an allegation of Discrimination, Harassment, or Bullying means advising a person in authority of the concern. Reporting a concern is not the filing of a Formal Complaint under this Procedure.

Allegations of Discrimination, Harassment, or Bullying can be reported to any of the following:

For employees:

- direct supervisors or managers;
- if the direct supervisor or manager is the subject of the reported behaviour, their manager;
- the Health and Safety Representative;
- the Human Resources Department
- the Senior Director Student Success or designate if the conduct is that of a student, per Policy 5102, Student Code of Conduct (Non-Academic);
- RDI; or,
- a Union Representative.

For students:

- Faculty and Faculty Instructors, Program or Department Heads, or Associate Deans;
- the Student Life Office;
- the Senior Director Student Success or designate, if the conduct is that of a student, per Policy 5102, Student Code of Conduct (Non-Academic);
- RDI; or,
- the Advocacy Services of the Student Association.

For anyone else:

- The supervisor or manager of the person whose behaviour is being reported; or,
- RDI.

2. Addressing Concerns through the RDI Office

During an initial meeting with a person reporting potential violation of the Policy, RDI will outline the Policy and available options, provide advice regarding rights to representation and confidentiality, and discuss available resources for example those found on the RDI webpage.

(a) Informal Resolution Process

RDI may, if appropriate, offer to address the reported potential violation informally, without the filing of a Formal Complaint. An offer to assist an Informal Resolution is not a determination as to the merits of the case.

Informal Resolution is a voluntary process. Parties are strongly encouraged to make a reasonable effort to resolve matters unless they feel unsafe doing so. Any party to the concern may decline to participate in this process or may terminate their participation in the process at any time without prejudice. Informal Resolution may take various forms, including but not limited to:

- RDI relaying a concern brought by one party about another and providing information around behavioural expectations set out in the Policy;
- exchanging information between the parties to facilitate resolution; and,
- bringing parties together for facilitated conversations to resolve matters.

The Informal Resolution process is confidential. Any statements made in good faith in attempting to resolve the matter, including apologies (in accordance with the *Apology Act*) or admissions of culpability cannot be used against either party should the matter proceed to a Formal Complaint and Investigation.

If an Informal Resolution is not initiated or does not resolve the matter, the Complainant may submit a Formal Complaint in accordance with this Procedure.

(b) Formal Complaints

(i) *Documenting a Formal Complaint*

Potential Complainants are strongly encouraged to discuss their concerns with RDI before submitting a Formal Complaint.

Any person filing a Formal Complaint must do so in good faith. A Formal Complaint must be provided in the prescribed manner or equivalent as determined by RDI. This includes filing the appropriate complaint form and providing information clearly outlining:

- name of the person submitting the Complaint (Complainant);
- name of the person(s) alleged to have breached the Policy (Respondent(s)), or if not yet known, a sufficiently clear description of the person(s), their apparent role, and circumstances, to enable identification;
- The specific sections of the Policy that are believed to have been breached;
- the actions, comments, behavior, or decisions believed to have contravened the Policy; and,
- a timeline of relevant events.

(ii) *Submitting a Formal Complaint*

A Formal Complaint can usually be submitted only by the person who was subjected to the alleged prohibited conduct. Exceptions where others may file a Formal Complaint may include:

- Complaints alleging systemic discrimination;
- Complaints filed on another's behalf with their signed consent (subject to collective agreement provisions); or,
- Complaints where in the opinion of the Head of RDI extenuating circumstances warrant acceptance.

A Complainant is required to inform RDI if they have reason to believe this matter has been, is being, or will be addressed through another complaint process either internally or externally.

(iii) *Review of Filed Formal Complaint*

RDI reviews all filed Formal Complaints to determine whether to accept them. They may decline to accept a Formal Complaint on any of the following grounds:

- the allegations are so unclear or vague that they could not be reasonably dealt with in accordance with procedural fairness;
- the allegations are past the time limit specified in the Policy and an extension has not been granted;
- the allegations (even if assumed to be true) do not constitute behaviour prohibited by the Policy;
- the allegations have been or are being fairly dealt with through another suitable process or proceeding;
- if doing so may prejudice the rights of a party to a Complaint in another proceeding; and,
- any other reason, if in accordance with procedural fairness.

If RDI declines the Complaint, they will advise the Complainant in writing, within 15 working days or notify them that more time is required to decide. They will also refer the Complainant to other BCIT policies that may address the matter, or to other BCIT services or supports, or to services outside BCIT that may assist in resolving the concerns.

The Complainant may request a review of RDI's decision to decline the Complaint. The Head of RDI must review the Formal Complaint within 10 working days of the request and advise the Complainant in writing of their decision.

If the reviewer determines to uphold the decision to decline the Complaint, the Complainant will be notified and no further action will be taken by RDI with respect to the Formal Complaint. The Complainant may pursue other available internal or external processes.

If, after review, the reviewer accepts the Formal Complaint, RDI will proceed in the manner outlined below.

(iv) *Acceptance of a Formal Complaint*

When RDI accepts a Formal Complaint, it will advise the Complainant. Acceptance of a Formal Complaint does not mean that it has been determined that the Complaint has merit.

The Complainant may request Formal Resolution or an Investigation of the Complaint at any stage in the process.

RDI will provide a copy of the Formal Complaint to the Respondent(s) and advise them whether the Complainant is seeking a Formal Resolution of the matter or has requested an Investigation.

The Respondent is provided the opportunity to submit a Reply document, which will be shared with the Complainant.

(v) *Formal Resolution Process*

A Formal Resolution process can be initiated with the endorsement of RDI and the agreement of both the Complainant and the Respondent. This process is voluntary and either party, or RDI, can end it at any time, without prejudice.

The Formal Resolution Process can take several forms, including but not limited to facilitated conversations. RDI will outline for the parties the process involved and only proceed with agreement of both parties.

The resolution process is confidential. Any statements made in good faith attempts to resolve the matter, including an apology (in accordance with the *Apology Act*) or admittance of culpability cannot be used against either party should the matter later proceed to an Investigation and adjudication.

(vi) *Agreement Reached*

If a resolution is reached RDI can assist the parties in documenting a binding resolution. A resolution agreed to by the parties is considered to have addressed the Formal Complaint and resolved the matter. Copies of the documented resolution will be provided to both parties and be kept by RDI.

Where the resolution of the Formal Complaint is based on remedial measures agreed to by the Complainant and the Respondent, RDI can assist in the implementation of such measures.

Implementation of a resolution may require the sharing of information otherwise considered confidential by RDI. RDI will obtain the consent of both Complainant and Respondent if this is required.

(vii) *Agreement Violated*

Failure by the Complainant or Respondent to undertake remedial measures or adhere to the terms of the resolution may be regarded as a breach of the agreement and result in discipline or corrective action. RDI may refer a party's alleged breach of a resolution agreement to BCIT Labour Relations or to the Senior Director Student Success or designate for further review and to determine appropriate steps.

(c) Investigation

If a Formal Resolution process has not been attempted or was unsuccessful, the Complainant may request an Investigation.

(i) *Investigation Process*

RDI will conduct or administer the Investigation. Individuals who facilitated an attempted resolution will not be assigned as Investigators.

The Investigator is not an advocate but rather a neutral fact finder. The Investigation will determine whether, on a balance of probabilities, the Policy has been breached, as alleged in the Formal Complaint.

Both the Complainant and the Respondent will have the opportunity to provide any information and evidence they deem relevant, as well as to identify witnesses.

The Investigator will provide the Complainant and the Respondent with an opportunity to participate in at least one interview. All parties to a complaint will be given the opportunity to fully explain what happened from their perspective, to have their explanations and concerns fully considered, and to challenge evidence that is being considered, orally, in writing, or both.

Complainants and Respondents are expected to participate in the Investigation process, including one or more interviews. However, in cases where the Respondent fails to agree to an interview request within a reasonable time without appropriate justification, the Investigation will proceed without their participation. In cases where the Complainant fails to participate within a reasonable time without appropriate justification, or ceases to participate, RDI will determine whether the Investigation will proceed without their further participation or be terminated.

(ii) *Investigation Report*

At the conclusion of the Investigation the Investigator will produce a Report containing:

a. A summary of the Complainant's and Respondent's positions.
b. Findings of fact and reasons for that finding.
c. A determination as to whether the Policy was, on the balance of probabilities, breached and reasons for that finding.
d. If applicable, mitigating or aggravating factors relevant to the determination of potential discipline or corrective action if the Investigator determines a breach of the Policy has occurred.
e. If applicable, remedial suggestions regarding the specific circumstances of the Complaint and the maintenance of a respectful environment free of Discrimination, Harassment, and Bullying.

Copies of the Investigation Report will be provided to the Complainant and the Respondent. They may share it with their Representatives but with no one else, unless required by law.

(iii) *Breach of Policy and Discipline*

If the Investigation finds a breach of the Policy occurred, the Report will be forwarded to the appropriate Office to determine the next steps.

- If an employee is found to have breached the Policy, the Report will be forwarded to the Manager of Labour Relations for review:
    - The Manager of Labour Relations or their designate will follow established disciplinary processes in accordance with relevant collective agreements, policies, and legislation.
    - Employees have the right to grieve or contest discipline in accordance with applicable collective agreements, contracts, policies, and legislation.
- If a student is found to have breached the Policy, the report will be forwarded to the Senior Director of Student Success for review and to determine the appropriate outcome or discipline:
    - The Senior Director of Student Success, or their designate, will follow established disciplinary processes in accordance with relevant policies and legislation.
    - Students have the right to appeal discipline issued in accordance with the applicable policies (such as Policy 5102, Student Code of Conduct) and legislation.
- If the person who breached the Policy is neither a student nor employee RDI will determine what department should receive the Report to decide upon appropriate sanctions, if applicable.

In all cases where a violation of the Policy has occurred, BCIT will mitigate the impact of the incident by taking actions to restore a respectful working and learning environment and implementing measures to reduce the likelihood of recurrence.

A breach of confidentiality may result in referral to another department for further action.

3. Appeal to Board of Inquiry

(a) *Requesting Appeal to Board of Inquiry*

(i) Complainants or Respondents seeking to appeal Investigation findings to a Board of Inquiry (“applicant”) must submit a request in writing to RDI, setting out the reasons for an Appeal. The applicant must do so within 10 working days of receipt of the Investigation Report. They are also responsible for notifying their Representative of the request and disclosing a copy of the Investigation Report to them. In the case of excluded staff, they must notify the Manager of Labour Relations.

(ii) The applicant’s Representative (or the Manager of Labour Relations) may notify RDI of

the request in writing within 20 working days of receipt of the Report (or a longer period as mutually agreed by the Representatives of the Complainant and the Respondent) that an Appeal is being requested.

(iii) If no such request (above) is received, the findings of the Investigator shall be determinative of the Complaint.

(iv) Upon receipt of the Notice, the Head of RDI shall advise the President in writing that a Board of Inquiry is required.

(b) *Board of Inquiry*

(i) Upon receipt of the Notice the Head of RDI will, within five working days, inform an available Arbitrator mutually agreed upon by the Representatives of the parties.

(ii) The Arbitrator selected shall make every effort to convene a Board of Inquiry within thirty working days.

(iii) The Board of Inquiry will conduct a hearing at which the Complainant, the Respondent, their Representatives, and BCIT are present. The Board of Inquiry hearing shall be conducted in a procedurally fair manner and held in private.

(iv) The Board of Inquiry shall determine its own procedures and advise the parties of them before the Inquiry begins. The Board of Inquiry may consider any evidence it deems necessary or appropriate if the consideration of that evidence is consistent with procedural fairness.

(v) The Board of Inquiry shall prepare a written decision within ten working days of the conclusion of the hearing, summarizing the facts and evidence considered, the decision of the Board of Inquiry as to whether Discrimination, Harassment, or Bullying occurred, and the reasons for that determination.

(vi) The Board of Inquiry may make any other order or any other recommendation it deems appropriate to correct the situation of Discrimination, Harassment, or Bullying, and that order shall form part of the written decision.

(vii) The decision of the Board of Inquiry as to whether Discrimination, Harassment, or Bullying occurred, and including any orders that the Board of Inquiry makes to resolve or remedy the matter, shall be final and binding on BCIT, the Complainant, the Respondent, and their Representatives.

(viii) The Board of Inquiry shall deliver its written decision within ten working days of the conclusion of the hearing to the:

- Complainant;
- Respondent;
- President;
- Head of RDI;
- Manager of Labour Relations, where any party is an employee;
- Bargaining unit staff representative, where any party is a member of a bargaining unit;
- Senior Director Student Success, if any party is a students; and,
- the Registrar, if any party is a student.

4. Appeal to Board of Governors

(a) A student disciplined under this Policy has a right pursuant to Section 37(2) of the *College and Institute Act* to appeal to the Board of Governors. In such an appeal, a decision by the Board of Governors regarding the discipline is final and determinative. By electing to appeal to the Board of Governors, the student is precluded from review of the discipline by a Board of Inquiry.

(b) An employee suspended under this Policy has a right pursuant to Section 37(1) of the *College and Institute Act* to appeal to the Board of Governors. In such an appeal, a decision by the Board of Governors regarding the suspension is final and determinative. By electing to appeal to the Board of Governors, the employee is precluded from review of the suspension by a Board of Inquiry.

Other Information

1. Grievance and Arbitration

(a) BCIT, the British Columbia General Employees' Union (BCGEU) Support Bargaining Unit, BCGEU Faculty Bargaining Unit, and the BCIT Faculty and Staff Association (BCITFSA), agree that the Complaint and Investigation processes provided in this Policy and Procedure constitute the grievance process for all complaints of Discrimination, Harassment, and Bullying on grounds included in this policy and involving employees who are members of bargaining units.

In such cases employees shall not access any other grievance processes in the collective agreements.

(b) The aforementioned parties further agree that the Board of Inquiry in this Policy and Procedure is a Board of Arbitration under the *Labour Relations Code* of British Columbia, which will render when required a final and binding determination in all Complaints of Discrimination, Harassment, and Bullying involving employees who are members of bargaining units.

2. Conflict of Interest

(a) If, at the outset of a Formal Resolution or Investigation, the Complainant or Respondent or their Representative believe RDI to be in a conflict of interest, they will document their concern and advise RDI. A copy will be shared with the other party to the Complaint, who has the right to respond.

(b) For the purposes of this Policy a conflict of interest exists when there is clear and convincing evidence that the RDI representative has a personal or professional interest which is sufficient to influence or appear to influence the objective exercise or proper discharge of their duties. A conflict of interest situation may arise even where there is no intention of acting unfairly or dishonestly. The fact that a conflict of interest is alleged does not in itself create such a conflict.

(c) If the Head of RDI agrees there is a conflict of interest they will reassign the file. If they do not agree, the Resolution or Complaint process may proceed with the original file assignment.

(d) If the Head of RDI is alleged to have a conflict of interest, but disagrees, the individual alleging the conflict may request the Steering Committee to consider whether a conflict of interest exists for the purpose of file reassignment.

3. Withdrawal of Complaint

A Complainant may withdraw their Complaint at any time by notifying RDI.

Withdrawal of a Complaint does not prevent a Respondent from filing a Complaint alleging the initial Complaint was frivolous, vexatious, malicious, or in bad faith.

4. Interim Measures

(a) If RDI determines that interim measures are appropriate to protect the health or safety, including psychological safety, of anyone involved; or to protect the integrity of an Investigation, they may require implementation of appropriate interim measures by persons with authority to do so.

(b) Interim measures may require the sharing of information which would otherwise be considered confidential. Only information needed to protect safety will be shared.

(c) Interim measures may include but are not limited to taking steps to prevent involved individuals from interacting with each other, such as by altering learning or working schedules or locations. Any interim measure will not impact the outcome of a complaint.

Forms Associated with This Procedure

None

Amendment History

		Approval Date	Status
Created:	7507 Procedure PR1 version 1	2009 May 01	Replaced
Revised:	7507 Procedure PR1 version 2	2010 June 29	Replaced
Revised:	7507 Procedure PR1 version 3	2014 July 22	In force
Revised:	7507 Procedure PR1 version 4 [draft]	*tbd*	In review

Scheduled Review Date

TBD [approval date + 5 years; or earlier, if regulatory or operational changes require review. The parties may at any time – by mutual agreement – initiate draft amendments for consideration by the Board for approval.]

PREVENTION OF DISCRIMINATION, HARASSMENT, AND BULLYING – PROCEDURE #7507-PR1

REDLINE

Prevention of Discrimination, Harassment, and Bullying ~~Harassment and Discrimination~~

Procedure No.:	7507-PR1
Version:	4
Policy Reference:	7507, Prevention of Discrimination, Harassment, and Bullying
Category:	~~Administration~~
Approval Body:	Board of Governors
Executive Sponsor:	VP People, Culture, & Inclusion
Department Responsible:	~~Harassment and Discrimination Advisor~~ People Culture, & Inclusion (Respect, Diversity, & Inclusion Office)
Directory of Records Class:	0650-10
~~Current~~ Approval~~ed~~ Date:	~~2014 Jul 22~~TBD

Objectives

This procedure applies directly to Policy 7507, Prevention of ~~Harassment and~~ Discrimination, Harassment, and Bullying. This procedure provides a fair and equitable process for the resolution of concerns and Formal (written or otherwise document) complaints of ~~Bullying and Harassment and~~ Discrimination, Harassment, or Bullying (including retaliation as defined in the Policy)~~, enabling Bullying and Harassment or Discrimination to be stopped as soon as it occurs.~~

Who ~~Does~~ This Procedure Applies~~y~~ To?

This procedure applies to all BCIT students, employees, contractors, volunteers, visitors, and members of the Board of Governors, during all BCIT-related activities. ~~and contract employees.~~

Scope

BCIT-related activity includes any type of activity or communication directly related to or arising out of the operations of BCIT regardless of the location, including but not limited to: online and electronic communications; engagement with the public; practicums; field schools; co-ops; conferences; BCIT-sponsored events; participation in student clubs, teams, and social events sponsored by the Student Association or its clubs.

Purpose

The purposes of this Procedure are:

- to communicate how concerns relating to conduct prohibited under the Policy are to be addressed; and,
- to set out the roles, rights, and responsibilities of parties to a Complaint.

Related Documents and Legislation

As set out in the Policy.

Definitions

The terms and meanings in this Procedure are as used and defined in the Policy

Table of Contents

Individuals are encouraged to resolve concerns informally, if they feel safe doing so. An individual may directly advise a person they believe has behaved inappropriately that the behaviour is unwelcome.

Any individual who believes they have been or are being subjected to Discrimination, Harassment, or Bullying as defined in Policy 7507 should keep a record of the incident or incidents of the prohibited behaviour including dates, times, what happened, and names of any witnesses.

All *employees* are expected to report any behaviour that they believe could constitute Bullying and Harassment to a person in authority, even if they do not wish to make a Formal Complaint.

Members of the BCIT community are strongly encouraged to report any instances of suspected Discrimination, Harassment, or Bullying to a person in authority, especially if they or others have been unable to resolve it directly.

BCIT personnel who manage or supervise employees have an obligation to take reasonable steps within their scope of authority to prevent and respond to Discrimination, Harassment, or Bullying they are aware of.

Faculty and Faculty Instructors responsible for students have an obligation to take reasonable steps within the scope of their authority to prevent and respond to Discrimination, Harassment, or Bullying of their students they are aware of.

All employees are encouraged to contact RDI with any questions about how to fulfill their responsibilities.

Anyone believing or suspecting that Policy 7507 may have been breached, whether or not they are the individual subjected to the conduct in question, can contact RDI for confidential advice and information.

RDI will listen to the concern raised, ask questions, and provide relevant information appropriate to the situation. Such advice or information may include an assessment of whether the alleged behaviour appears to be conduct prohibited by the Policy, options for resolutions under this Procedure or other ways of addressing the concerns, and any referrals deemed appropriate.

RDI does not provide legal advice, nor does it advocate for any party.

Reporting an allegation of Discrimination, Harassment, or Bullying means advising a person in authority of the concern. Reporting a concern is not the filing of a Formal Complaint under this Procedure.

Allegations of Discrimination, Harassment, or Bullying can be reported to any of the following:

For employees:

- direct supervisors or managers;
- if the direct supervisor or manager is the subject of the reported behaviour, their manager;
- the Health and Safety Representative;
- the Human Resources Department
- the Senior Director Student Success or designate if the conduct is that of a student, per Policy 5102, Student Code of Conduct (Non-Academic);
- RDI; or,
- a Union Representative.

For students:

- Faculty and Faculty Instructors, Program or Department Heads, or Associate Deans;
- the Student Life Office;
- the Senior Director Student Success or designate, if the conduct is that of a student, per Policy 5102, Student Code of Conduct (Non-Academic);
- RDI; or,
- the Advocacy Services of the Student Association.

For anyone else:

- The supervisor or manager of the person whose behaviour is being reported; or,
- RDI.

2. Addressing Concerns through the RDI Office

During an initial meeting with a person reporting potential violation of the Policy, RDI will outline the Policy and available options, provide advice regarding rights to representation and confidentiality, and discuss available resources for example those found on the RDI webpage.

(a) Informal Resolution Process

RDI may, if appropriate, offer to address the reported potential violation informally, without the filing of a Formal Complaint. An offer to assist an Informal Resolution is not a determination as to the merits of the case. Informal Resolution is a voluntary process. Parties are strongly encouraged to make a reasonable effort to resolve matters unless they feel unsafe doing so. Any party to the concern may decline to participate in this process or may terminate their participation in the process at any time without prejudice. Informal Resolution may take various forms, including but not limited to:

- RDI relaying a concern brought by one party about another and providing information around behavioural expectations set out in the Policy;
- exchanging information between the parties to facilitate resolution; and,
- bringing parties together for facilitated conversations to resolve matters.

The Informal Resolution process is confidential. Any statements made in good faith in attempting to resolve the matter, including apologies (in accordance with the Apology Act) or admissions of culpability cannot be used against either party should the matter proceed to a Formal Complaint and Investigation. If an Informal Resolution is not initiated or does not resolve the matter, the Complainant may submit a Formal Complaint in accordance with this Procedure.

(b) Formal Complaints

(i) Documenting a Formal Complaint

Potential Complainants are strongly encouraged to discuss their concerns with RDI before submitting a Formal Complaint.

Any person filing a Formal Complaint must do so in good faith. A Formal Complaint must be provided in the prescribed manner or equivalent as determined by RDI. This includes filing the appropriate complaint form and providing information clearly outlining:

• name of the person submitting the Complaint (Complainant);
• name of the person(s) alleged to have breached the Policy (Respondent(s)), or if not yet known, a sufficiently clear description of the person(s), their apparent role, and circumstances, to enable identification;
• the specific sections of the Policy that are believed to have been breached;
• the actions, comments, behavior, or decisions believed to have contravened the Policy; and,
• a timeline of relevant events.

(ii) Submitting a Formal Complaint

A Formal Complaint can usually be submitted only by the person who was subjected to the alleged prohibited conduct. Exceptions where others may file a Formal Complaint may include:

• Complaints alleging systemic discrimination;
• Complaints filed on another's behalf with their signed consent (subject to collective agreement provisions); or,
• Complaints where in the opinion of the Head of RDI extenuating circumstances warrant acceptance.

A Complainant is required to inform RDI if they have reason to believe this matter has been, is being, or will be addressed through another complaint process either internally or externally.

~~**Procedure to Resolve a Complaint of Harassment and/or Discrimination**~~

~~1. Members of the BCIT community are encouraged whenever possible to resolve problems informally and, where necessary, to request the Harassment and Discrimination Advisor (Advisor) to advise and assist in this process.~~

~~2. An individual who believes they are being subjected to Bullying and Harassment or Discrimination as defined in Policy 7507, Harassment and Discrimination (the Complainant) should keep a written record of the incident or incidents of the Bullying, Harassment or Discrimination including such information as dates, times, what happened, and names of witnesses, if any.~~

~~3. An individual is encouraged to advise the person they believe has bullied, harassed them or discriminated against them (the Respondent) that the behaviour is unacceptable and ask them to stop. If this is too intimidating or inappropriate, or if the attempt to stop the offending behaviour is unsuccessful, the Complainant may seek the advice of the Advisor.~~

~~4. If the perceived Bullying and Harassment or Discrimination persists, or the perceived Discrimination is systemic or relates to an Institute policy, the Complainant should speak to any of the following:~~

- ~~The Harassment and Discrimination Advisor (the Advisor).~~
- ~~Where the Complainant is a student, the Instructor, Program Head, Chief Instructor, Associate Dean, Registrar, a Counsellor, and/or Vice President of Student Affairs or the Director of the Student Association.~~
- ~~Where the Complainant is an employee, their supervisor, or where the supervisor is the alleged harasser, the manager the supervisor reports to.~~
- ~~Where the Complainant is a member of a bargaining unit, they may also wish to speak to their~~

~~shop steward or individual responsible for human rights within their bargaining unit.~~

~~5. Instructors, chief instructors, program heads, associate deans, the Registrar, counsellors, the vice-president, Vice President Academic or the Director of the Student Association, supervisors, managers, or bargaining unit representatives who have been approached by a Complainant may contact the Harassment and Discrimination Advisor in confidence for advice on how to proceed, or they may refer the Complainant to the Harassment and Discrimination Advisor.~~

(iii) Review of Filed Formal Complaint

RDI reviews all filed Formal Complaints to determine whether to accept them. They may decline to accept a Formal Complaint on any of the following grounds:

- the allegations are so unclear or vague that they could not be reasonably dealt with in accordance with procedural fairness;
- the allegations are past the time limit specified in the Policy and an extension has not been granted;
- the allegations(even if assumed to be true) do not constitute behaviour prohibited by the Policy;
- the allegations have been or are being fairly dealt with through another suitable process or proceeding;
- if doing so may prejudice the rights of a party to a Complaint in another proceeding; and,
- any other reason, if in accordance with procedural fairness.

If RDI declines the Complaint, they will advise the Complainant in writing, within 15 working days or notify them that more time is required to decide. They will also refer the Complainant to other BCIT policies that may address the atter, or to other BCIT services or supports, or to services outside BCIT that may assist in resolving the concerns.

The Complainant may request a review of RDI's decision to decline the Complaint. The Head of RDI must review the Formal Complaint within 10 working days of the request and advise the Complainant in writing of their decision.

If the reviewer determines to uphold the decision to decline the Complaint, the Complainant will be notified and no further action will be taken by RDI with respect to the Formal Complaint. The Complainant may pursue other available internal or external processes.

If, after review, the reviewer accepts the Formal Complaint, RDI will proceed in the manner outlined below.

(iv) Acceptance of a Formal Complaint

When RDI accepts a Formal Complaint, it will advise the Complainant. Acceptance of a Formal Complaint does not mean that it has been determined that the Complaint has merit.

The Complainant may request Formal Resolution or an Investigation of the Complaint at any stage in the process.

RDI will provide a copy of the Formal Complaint to the Respondent(s) and advise them whether the Complainant is seeking a Formal Resolution of the matter or has requested an Investigation.

The Respondent is provided the opportunity to submit a Reply document, which will be shared with the Complainant

~~**Initiating a Complaint – Initial Meetings with the Advisor**~~

6. ~~During the initial meeting with the Complainant, the Advisor will outline the policy, coverage, and criteria and the options available for resolving complaints. As well the Advisor will advise the Complainant about their right to representation and confidentiality. The Advisor will also discuss resources such as Employee & Family Assistance Plan (EFAP) if in the opinion of the Advisor the~~

~~Complainant would benefit from such advice.~~

~~7. The parties to Policy 7507, Harassment and Discrimination recognize that there may be circumstances when it is inappropriate for the Advisor to act in this capacity for a specific complaint due to a conflict of interest.~~

~~For the purposes of Policy 7507, a conflict of interest exists when there is clear and convincing evidence that the Advisor has (or may be perceived to have) a personal or professional interest in the outcome or resolution of the complaint. If, at the outset, the Complainant or Respondent believes the Advisor to be in a conflict of interest situation, they shall so advise the Advisor. If the Advisor does not agree that a conflict of interest exists, the Complainant or Respondent may request that an alternate Advisor be appointed to implement Policy 7507.~~

~~In that case, the Complainant or Respondent must submit their request to the President of the relevant BCGEU bargaining unit (if they are a member of a bargaining unit), the Vice President of Student Affairs or Director of the Student Association (if they are a student), or the Manager of Labour Relations (if they are an excluded employee). The representative may submit a written request for an alternate Advisor. The written request must state the reason for the request.~~

~~8. If the Advisor receives a request from the Complainant's representative or theRespondent's representative that an alternate Advisor be appointed, the steering committee will be convened and will review the request for an alternate Advisor. If the steering committee agrees that a conflict of interest exists, an appointment of an alternate Advisor will be made from a list (Schedule A) of mutually agreed alternate Advisors. The appointment will be made from the list in the order that appears on the list. The alternate Advisor will conduct a review of the complaint in accordance with Sections 9–20 of these procedures. The list may be amended from time to time with the agreement of all of the parties to Policy 7507.~~

~~9. If the Complainant wishes to pursue the resolution of the complaint, the Advisor will:~~

- ~~Interview the Complainant to obtain all factual information including dates, times, and what happened from the Complainant's point of view, the name of the Respondent, and the names of any witnesses.~~
- ~~Obtain a written complaint from the Complainant in which the details of the allegations are clearly described.~~
- ~~Determine whether the complaint fits within one or more definitions of Bullying and Harassment and Discrimination as defined in Policy 7507, and determine whether the complaint falls within the timelines set out in Section 3, "Time Limit", of the Duties, Responsibilities and General Information Section of Policy 7507. This determination is a *prima facie* determination only and does not constitute a finding about the merits of the complaint or the accuracy of the facts alleged.~~

~~**10.** The Advisor will advise the Complainant of the determination within two (2) working days of the initial meeting with the Complainant.~~

~~**11.**If the complaint does not fall within the definitions or time limit of Policy 7507, the Advisor will:~~

- ~~So advise the Complainant and, if requested, will provide reason(s) in writing.~~
- ~~Refer the Complainant to other BCIT policies which may address the matter, or to other BCIT services, or to services outside BCIT which may provide assistance in resolving the complaint.~~

~~**12.**If the Advisor concludes pursuant to Section 9 above that the complaint does not fall within the definitions or time limit of Policy 7507, the Complainant may request a review of that finding by an alternate Advisor selected from Schedule A. The alternate Advisor shall review the complaint within 10 working days of their appointment.~~

~~**13.**~~9. ~~In the event the alternate Advisor finds that the complaint does fall within the definitions or time limit of Policy7507, the complaint will be referred back to the Advisor who shall attempt to resolve the complaint in accordance with the procedures that follow.~~

Options for Resolving a Complaint

14. If the Advisor determines that the complaint fits within the definitions of the policy, consideration must be given to resolving the complaint through an informal resolution process. The Advisor will suggest this option to the Complainant.

If the Complainant agrees to attempt to resolve the complaint informally, the Advisor will:

- Interview the Complainant to obtain any additional information required to facilitate the resolution process.
- Advise the Respondent of the complaint and obtain all factual information about dates, time, and what happened from the Respondent's point of view.
- Outline the policy, coverage, and criteria and the options available for resolving complaints to the Complainant and Respondent.
- Advise the Respondent about their right to representation, confidentiality, and resources such as Employee & Family Assistance Plan (EFAP), if in the opinion of the Advisor the Respondent would benefit from such advice.
- Advise the Complainant and the Respondent of the process to be used to resolve the complaint and obtain their consent to the process.

15. Procedures for resolving complaints informally may vary according to the circumstances of the complaint at the discretion of the Advisor. Such proceedings may include an attempt to informally resolve the matter through problem solving and mediation. If the Complainant and the Respondent cannot reach agreement at the end of the informal process, or do not agree to proceed with an informal process, the Advisor will conduct an investigation in accordance with the process set out herein and the principles of procedural fairness. Investigations will typically include interviews with the Complainant, Respondent and applicable witnesses. At the conclusion of the investigation the Advisor will prepare a short, written report (the Report) of the investigation that includes the following:

- In the opinion of the Advisor, whether Bullying and Harassment and/or Discrimination as defined by Policy 7507 occurred;
- The reasons for this opinion;
- Recommendations, where appropriate, regarding the creation of an effective working environment, one that is free of harassment and discrimination;
- The Complainant and Respondent may indicate their acceptance of the terms of the resolution by signing the Report.

The Advisor may inform the appropriate manager of the complaint, only if by informing the manager a resolution will be more likely. This step will only be done with the knowledge of the Complainant and the Respondent.

16. If, for any reason, the attempt at informal resolution has been unsuccessful, the Advisor's Report shall so indicate, and the Complainant and the Respondent will sign the Report to acknowledge receipt and that the attempt at resolution has been made. The Report will include the reasons for the unsuccessful conclusion. The Complainant may then choose one of the other options listed under Section 20.

17. A copy of the Report of the Advisor shall be provided to the Complainant and the Respondent and shall remain confidential. If the Respondent is an employee and discipline is recommended, a copy of the Report will be forwarded to the Manager of Labour Relations. If the Respondent is a student and discipline is recommended, a copy of the Report will be forwarded to the Office of the Registrar. When the Advisor recommends discipline and the Respondent is an employee, the Manager of Labour Relations will follow its usual process and determine the appropriate discipline, if any. The outcome will be communicated to the employee and the Respondent's representative and a copy of the Advisor's

~~Report will be sent to the Respondent's representative.~~

~~When the Advisor recommends discipline and the Respondent is a student, the Registrar will determine the appropriate discipline. The student will be advised what discipline is being imposed, and a copy of that letter and the Advisor's Report will be sent to the Respondent's representative.~~

~~18. Where the resolution process has involved a manager, a union representative, or a student representative, those individuals will be advised by the Advisor of the nature of the resolution to the complaint.~~

(v) Formal Resolution Process

A Formal Resolution process can be initiated with the endorsement of RDI and the agreement of both the Complainant and the Respondent. This process is voluntary and either party, or RDI, can end it at any time, without prejudice.

The Formal Resolution Process can take several forms, including but not limited to facilitated conversations. RDI will outline for the parties the process involved and only proceed with agreement of both parties.

The resolution process is confidential. Any statements made in good faith attempts to resolve the matter, including an apology (in accordance with the Apology Act) or admittance of culpability cannot be used against either party should the matter later proceed to an Investigation and adjudication.

(vi) Agreement Reached

If a resolution is reached RDI can assist the parties in documenting a binding resolution. A resolution agreed to by the parties is considered to have addressed the Formal Complaint and resolved the matter. Copies of the documented resolution will be provided to both parties and be kept by RDI.

Where the resolution of the Formal Complaint is based on remedial measures agreed to by the Complainant and the Respondent, RDI can assist in the implementation of such measures.

Implementation of a resolution may require the sharing of information otherwise considered confidential by RDI. RDI will obtain the consent of both Complainant and Respondent if this is required.

(vii) Agreement Violated

Failure by the Complainant or Respondent to undertake remedial measures or adhere to the terms of the resolution may be regarded as a breach of the agreement and result in discipline or corrective action. RDI may refer a party's alleged breach of a resolution agreement to BCIT Labour Relations or to the Senior Director Student Success or designate for further review and to determine appropriate steps

~~19. Where the resolution of the complaint is based on remedial measures agreed to by the Complainant and the Respondent, the Advisor will make the necessary arrangements for the implementation of such measures. Failure of the Complainant or the Respondent to undertake remedial measures outlined in the agreement will be regarded as a breach of the agreement and may be considered grounds for discipline or to reopen the complaint.~~

~~20. If the informal process is unsuccessful and after the Complainant and Respondent have received the Report, the Complainant or Respondent may proceed as follows:~~

- ~~Take no further action.~~
- ~~Resolve the matter themselves.~~
- ~~Request the appointment of a Board of Inquiry.~~
- ~~Pursue any other course of action available at law, under a collective agreement, or pursuant to other~~

~~Institute policies and procedures.~~

~~Where the Complainant or Respondent requests a Board of Inquiry, the request must be submitted in writing to the Advisor and their representative within 10 working days of receipt of the Advisor's Report. The Advisor will notify the Complainant's representative or the Respondent's representative of the request.~~

(c) Investigation

If a Formal Resolution process has not been attempted or was unsuccessful, the Complainant may request an Investigation.

(i) Investigation Process

RDI will conduct or administer the Investigation. Individuals who facilitated an attempted resolution will not be assigned as Investigators.

The Investigator is not an advocate but rather a neutral fact finder. The Investigation will determine whether, on a balance of probabilities, the Policy has been breached, as alleged in the Formal Complaint.

Both the Complainant and the Respondent will have the opportunity to provide any information and evidence they deem relevant, as well as to identify witnesses.

The Investigator will provide the Complainant and the Respondent with an opportunity to participate in at least one interview. All parties to a complaint will be given the opportunity to fully explain what happened from their perspective, to have their explanations and concerns fully considered, and to challenge evidence that is being considered, orally, in writing, or both.

Complainants and Respondents are expected to participate in the Investigation process, including one or more interviews. However, in cases where the Respondent fails to agree to an interview request within a reasonable time without appropriate justification, the Investigation will proceed without their participation. In cases where the Complainant fails to participate within a reasonable time without appropriate justification, or ceases to participate, RDI will determine whether the Investigation will proceed without their further participation or be terminated.

(ii) Investigation Report

At the conclusion of the Investigation the Investigator will produce a Report containing:

a. A summary of the Complainant's and Respondent's positions.
b. Findings of fact and reasons for that finding.
c. A determination as to whether the Policy was, on the balance of probabilities, breached and reasons for that finding.
d. If applicable, mitigating or aggravating factors relevant to the determination of potential discipline or corrective action if the Investigator determines a breach of the Policy has occurred.
e. If applicable, remedial suggestions regarding the specific circumstances of the Complaint and the maintenance of a respectful environment free of Discrimination, Harassment, and Bullying.

Copies of the Investigation Report will be provided to the Complainant and the Respondent. They may share it with their Representatives but with no one else, unless required by law.

~~**Board of Inquiry**~~

~~21. The parties to Policy 7507 who are representatives of the Complainant or the Respondent, or the Manager of Labour Relations for excluded staff, may notify the Advisor in writing within 20 working days of receipt of the Report (or such longer period as is mutually agreed by the representatives of the Complainant and the Respondent) that a Board of Inquiry is required (the Notice). Such Notice shall set out the reasons for~~

~~an appeal to the Board of Inquiry. Decisions to proceed to a Board of Inquiry will be made in accordance with the usual practices of the Union, Labour Relations or the Student Association. If no such Notice is received, the findings and recommendations of the Advisor shall be determinative of the complaint.~~

~~22. Upon receipt of the Notice, the Advisor shall advise the President in writing that a Board of Inquiry is required.~~

~~23. Upon receipt of the Notice the Advisor will, within 5 working days, inform the next available person on the List of Arbitrators in Schedule B that they are to conduct a Board of Inquiry.~~

~~24. The List of Arbitrators in Schedule B has been mutually agreed to by BCIT, the BCGEU Local 703 Support and Instructional Bargaining Units, the BCIT Faculty and Staff Association, and the Student Association, and may be changed from time to time upon mutual agreement~~

~~25. The Arbitrator selected shall convene a Board of Inquiry within thirty (30) working days.'~~

~~26. The Board of Inquiry will conduct a hearing at which the Complainant, the Respondent, their representatives, and BCIT are present.~~

~~27. The Board of Inquiry shall be conducted in a manner consistent with the principles of natural justice and ensure that the Complainant and Respondent are given a fair hearing. The Board of Inquiry must be held in private.~~

~~28. The Board of Inquiry shall determine its own procedures and shall advise the parties of these procedures before the Inquiry begins. The Board of Inquiry may consider any evidence it deems necessary or appropriate as long as the consideration of that evidence is consistent with the principles of natural justice.~~

~~29. The Board of Inquiry shall prepare a written decision within 10 working days of the conclusion of the Board of Inquiry, which summarizes the facts and evidence considered, the decision of the Board of Inquiry as to whether harassment or discrimination occurred, and the reasons for that determination. The Board of Inquiry may make any other order or any other recommendation it deems appropriate to correct the situation of Bullying and Harassment or Discrimination, and that order shall form part of the written decision.~~

~~30. The decision of the Board as to whether Bullying and Harassment or Discrimination occurred, and including any orders that the Board of Inquiry makes to resolve the matter, shall be final and binding on BCIT, the Complainant, the Respondent, and their representatives.~~

~~31. The Board shall forward its written decision within ten (10) working days of the conclusion of the Inquiry to the:~~

- ~~Complainant.~~
- ~~Respondent.~~
- ~~President.~~
- ~~Advisor.~~
- ~~Manager of Labour Relations where any of the parties is an employee.~~
- ~~Bargaining unit staff representative where any of the parties is a member of a bargaining unit, or the Registrar where any of the parties is a student.~~

(iii) Breach of Policy and Discipline

If the Investigation finds a breach of the Policy occurred, the Report will be forwarded to the appropriate Office to determine the next steps.

- If an employee is found to have breached the Policy, the Report will be forwarded to the Manager of Labour Relations for review:
    - The Manager of Labour Relations or their designate will follow established disciplinary processes in

accordance with relevant collective agreements, policies, and legislation.
o Employees have the right to grieve or contest discipline in accordance with applicable collective agreements, contracts, policies, and legislation.

• If a student is found to have breached the Policy, the report will be forwarded to the Senior Director of Student Success for review and to determine the appropriate outcome or discipline:

o The Senior Director of Student Success, or their designate, will follow established disciplinary processes in accordance with relevant policies and legislation.
o Students have the right to appeal discipline issued in accordance with the applicable policies (such as Policy 5102, Student Code of Conduct) and legislation.

• If the person who breached the Policy is neither a student nor employee RDI will determine what department should receive the Report to decide upon appropriate sanctions, if applicable.

In all cases where a violation of the Policy has occurred, BCIT will mitigate the impact of the incident by taking actions to restore a respectful working and learning environment and implementing measures to reduce the likelihood of recurrence.

A breach of confidentiality may result in referral to another department for further action.

~~**Discipline**~~

~~32. Where a letter of discipline is to be placed on an employee's Personnel File, it shall be done in accordance with the relevant language of the appropriate collective agreement.~~

~~33. Where an employee requests the removal of any letters, referred to in Section 32 from the employee's Personnel File, this request shall be subject to the relevant language of the appropriate collective agreement, and shall be grievable in accordance with the relevant language of the appropriate collective agreement.~~

~~34. Where a letter of discipline is to be placed on a student's official record, the student shall be so notified in writing by the Registrar.~~

~~The student shall be entitled to a copy of all such letter(s), and to indicate by initialling the letter(s) that they have seen the letter(s). Such initialling shall in no way indicate concurrence with the content of the letter(s). The student shall also be entitled to add comments to such letter(s), or to add letters, documents, or materials to the file.~~

~~35. A student may request the removal of letters of discipline resulting from an informal or a formal resolution process under Policy 7507, two years after the date of such letter(s) being placed on the student's file, by forwarding a written request to the Registrar.~~

~~If the Registrar considers these letter(s) to be of continuing relevance, such a request may be denied in writing to the student. The Registrar shall not unreasonably refuse such a request.~~

~~The student shall have the right to appeal the decision of the Registrar to the Vice President of Student Services. When such letters of discipline have been removed from the student's file, the student shall be so notified in writing.~~

3. Appeal to Board of Inquiry

(a) Requesting Appeal to Board of Inquiry

(i) Complainants or Respondents seeking to appeal Investigation findings to a Board of Inquiry ("applicant") ~~Where the Complainant or Respondent requests a Board of Inquiry, the request~~ must be submit a request

~~ted~~ in writing to RDI, setting out the reasons for an Appeal. The applicant must do so ~~the Advisor and their representative~~ within 10 working days of receipt of the Investigation ~~Advisor's~~ Report. They are also responsible for notifying their Representative of the request and disclosing a copy of the Investigation Report to them. In the case of excluded staff, they must notify the Manager of Labor Relations. ~~The Advisor will notify the Complainant's representative or the Respondent's representative of the request.~~

(ii) The applicant's Representative (or the Manager of Labour Relations) ~~parties to Policy 7507 who are representatives of the Complainant or the Respondent, or the Manager of Labour Relations for excluded staff,~~ may notify RDI of the request ~~the Advisor~~ in writing within 20 working days of receipt of the Report (or a ~~such~~ longer period as is mutually agreed by the representatives of the Complainant and the Respondent) that an Appeal is being requested. ~~Board of Inquiry is required (the Notice). Such Notice shall set out the reasons for an appeal to the Board of Inquiry. Decisions to proceed to a Board of Inquiry will be made in accordance with the usual practices of the Union, Labour Relations or the Student Association.~~

(iii) If no such Notice is received, the findings and recommendations of the Advisor shall be determinative of the complaint.

(iv) Upon receipt of the Notice, the Advisor shall advise the President in writing that a Board of Inquiry is required.

(b) Board of Inquiry

(i) Upon receipt of the Notice the Head of RDI will, within five working days, inform an available Arbitrator mutually agreed upon by the Representatives of the parties. ~~The List of Arbitrators in Schedule B has been mutually agreed to by BCIT, the BCGEU Local 703 Support and Instructional Bargaining Units, the BCIT Faculty and Staff Association, and the Student Association, and may be changed from time to time upon mutual agreement~~

(ii) The Arbitrator selected shall make every effort to convene a Board of Inquiry within thirty ~~(30)~~ working days.~~'~~

(iii) The Board of Inquiry will conduct a hearing at which the Complainant, the Respondent, their representatives, and BCIT are present. The Board of Inquiry shall be conducted in a manner consistent with the principles of natural justice and ensure that the Complainant and Respondent are given a fair hearing. The Board of Inquiry must be held in private.

(iv) The Board of Inquiry shall determine its own procedures and shall advise the parties of these procedures before the Inquiry begins. The Board of Inquiry may consider any evidence it deems necessary or appropriate as long as the consideration of that evidence is consistent with procedural fairness ~~the principles of natural justice~~.

(v) The Board of Inquiry shall prepare a written decision within 10 working days of the conclusion of the hearing ~~Board of Inquiry, which summarizes~~ summarizing the facts and evidence considered, the decision of the Board of Inquiry as to whether Discrimination, Harassment, or Bullying occurred ~~harassment or discrimination occurred~~, and the reasons for that determination.

(vi) The Board of Inquiry may make any other order or any other recommendation it deems appropriate to correct the situation of Bullying and Harassment or Discrimination, and that order shall form part of the written decision.

(vii) The decision of the Board as to whether Bullying and Harassment or Discrimination occurred, and including any orders that the Board of Inquiry makes to resolve the matter, shall be final and binding on BCIT, the Complainant, the Respondent, and their representatives.

(viii) The Board shall forward its written decision within ten ~~(10)~~ working days of the conclusion of the Inquiry to the:

- Complainant;~~,~~
- Respondent;~~,~~

- President;~~.~~
- Head of RDI~~Advisor~~;~~.~~
- Manager of Labour Relations where any of the parties is an employee;~~.~~
- Bargaining unit staff representative, where any of the parties is a member of a bargaining unit;
- Senior Director Student Success, if any party is a student; and
- the~~, or the~~ Registrar, if ~~where~~ any ~~of the~~ party~~ies~~ is a student.

~~4.~~ Appeal to Board of Governors

(a) A student ~~who is~~ disciplined under this Policy has a right pursuant to Section 37(2) of the *Colleges and Institutes Act*~~, RSBC 1996, c.52 under this policy retains a right to appeal that discipline~~ to the Board of Governors. In such an appeal, ~~If a student elects to appeal discipline implemented under this policy to the Board of Governors,~~ a decision by the Board of Governors regarding the discipline is final and determinative ~~of the matter~~. As well, by electing to appeal to the Board of Governors, the student is precluded from pursuing a review of the discipline by a Board of Inquiry ~~on the matter of discipline~~.

(b) An employee~~, who is~~ suspended under this Policy has a right pursuant to Section 37(1) of the *Colleges and Institutes Act*~~, RSBC 1996, c.52 under this policy, retains a right~~ to appeal ~~that suspension~~ to the Board of Governors. In such an appeal ~~If the employee elects to appeal a suspension implemented as a form of discipline under this policy to the Board of Governors~~, a decision by the Board of Governors regarding the suspension is determinative ~~of the matter~~. ~~As well by~~By electing to appeal to the Board of Governors, the employee ~~member of the instructional, administrative and other staff~~ is precluded from pursuing a review of the suspension by a Board of Inquiry. ~~on the matter of the suspension~~

Other Information

1.Grievance and Arbitration

(a) BCIT, the British Columbia General Employees' Union (BCGEU) Support Bargaining Unit, BCGEU Faculty Bargaining Unit, and the BCIT Faculty and Staff Association (BCITFSA), agree that the Complaint and Investigation processes provided in this Policy and Procedure constitute the grievance process for all complaints of Discrimination, Harassment, and Bullying on grounds included in this policy and involving employees who are members of bargaining units.

In such cases employees shall not access any other grievance processes in the collective agreements.

(b) The aforementioned parties further agree that the Board of Inquiry in this Policy and Procedure is a Board of Arbitration under the Labour Relations Code of British Columbia, which will render when required a final and binding determination in all Complaints of Discrimination, Harassment, and Bullying involving employees who are members of bargaining units.

2. Conflict of Interest

(a) If, at the outset of a Formal Resolution or Investigation, the Complainant or Respondent or their Representative believe RDI to be in a conflict of interest, they will document their concern and advise RDI. A copy will be shared with the other party to the Complaint, who has the right to respond.

(b) For the purposes of this Policy a conflict of interest exists when there is clear and convincing evidence that the RDI representative has a personal or professional interest which is sufficient to influence or appear to influence the objective exercise or proper discharge of their duties. A conflict of interest situation may arise even where there is no intention of acting unfairly or dishonestly. The fact that a conflict of interest is alleged does not in itself create such a conflict.

(c) If the Head of RDI agrees there is a conflict of interest they will reassign the file. If they do not agree, the

Resolution or Complaint process may proceed with the original file assignment.

(d) If the Head of RDI is alleged to have a conflict of interest, but disagrees, the individual alleging the conflict may request the Steering Committee to consider whether a conflict of interest exists for the purpose of file reassignment

3. Withdrawal~~s~~ of Complaint~~s~~

~~36~~. A ~~The~~ Complainant may withdraw the complaint at any time by notifying RDI.~~the Advisor in writing.~~

Withdrawal of a Complaint does not prevent a Respondent from filing a Complaint alleging the initial Complaint was frivolous, vexatious, malicious, or in bad faith.

~~37. When a complaint is withdrawn prior to a determination being made of the validity of the Complainant's case, the Respondent, if they believe the complaint was vexatious or frivolous, has the right to initiate a complaint under Policy 7507 and these Procedures in order to have an opportunity to present their case.~~

4. Interim Measures ~~38. Health and Safety Measures~~

(a) If RDI determines that interim measures are appropriate to protect the health or safety, including psychological safety, of anyone involved; or to protect the integrity of an Investigation, they may require implementation of appropriate interim measures by persons with authority to do so.~~If at any time the Advisor believes that the personal or psychological safety of the Complainant or the Respondent are at risk, appropriate measures will be taken to protect the person, pending the outcome of an investigation and/or the resolution of the complaint.~~

(b) Interim measures may require the sharing of information which would otherwise be considered confidential. Only information needed to protect safety will be shared.

(c) Interim measures may include but are not limited to taking steps to prevent involved individuals from interacting with each other, such as by altering learning or working schedules or locations. Any interim measure will not impact the outcome of a complaint

~~If the Complainant or Respondent is a student, the Advisor will consult with the Registrar who will make the necessary arrangements to resolve safety issues.~~

~~If the Complainant or Respondent is an employee, the Advisor may consult the Manager of Labour Relations, the Manager of Human Resources, or the Director of Safety and Security for assistance in making the necessary arrangements to resolve the safety issue.~~

~~Such measures may involve the temporary relocation of one of the parties. The Complainant will not be relocated without their consent. Where temporary relocation is inappropriate or not possible, arrangements may be made for one of the parties to be placed on a leave of absence with pay until the complaint has been resolved.~~

Forms Associated With This Procedure

~~Schedule A, Alternate Advisors (in progress) Schedule B, List of Arbitrators (in progress)~~

None

Amendment History

	Approval Date	Status
Created: 7507 Procedure PR1 version 1	2009 May 01	Replaced
Revised: 7507 Procedure PR1 version 2	2010 June 29	Replaced
Revised: 7507 Procedure PR1 version 3	2014 July 22	In force
Revised: 7507 Procedure PR1 version 4 [draft]	tbd	In review
~~Created~~	~~2009 May 01~~	

~~1. Revision 1 2010 Jun 29~~
~~2. Revision 2 2014 Jul 22~~

Scheduled Review Date

TBD [approval date + 5 years; or earlier, if regulatory or operational changes require review. The parties may at any time – by mutual agreement – initiate draft amendments for consideration by the Board for approval.
~~2015 July~~

DECISION NOTE
November 20, 2025

PREPARED FOR: Board of Governors

PREPARED BY: Shawna Waberi, Chair, Education Council

ISSUE: New Programs:
- Certificate in Professional Remotely Piloted Aircraft Systems
- Diploma in Construction Management

APPENDICES:

1. Appendix A: Certificate in Professional Remotely Piloted Aircraft Systems – Business Plan
2. Appendix B: Certificate in Professional Remotely Piloted Aircraft Systems – Proposal (in Aprio)
3. Appendix C: Diploma in Construction Management – Business Plan
4. Appendix D: Diploma in Construction Management – Proposal (in Aprio)

RECOMMENDATION:

THAT the Board of Governors approves the following new programs: Certificate in Professional Remotely Piloted Aircraft Systems, and Diploma in Construction Management.

BACKGROUND:

At their respective meetings, the Education Council approved the new programs on November 19, 2025, and the Audit and Finance Committee approved same on November 18, 2025.

KEY ELEMENTS OF THE NEW PROGRAMS:

School of Transportation (SoT)
Certificate in Professional Remotely Piloted Aircraft Systems

The BCIT Certificate in Professional Remotely Piloted Aircraft Systems will meet the growing demand for skilled professionals in the rapidly evolving field of drone technology. This 18-week, 36-credit foundational program will offer students a comprehensive introduction to the technical, operational and regulatory aspects of drone operations. Upon completion students will be prepared to challenge exams to receive four Transport Canada certifications.

Curriculum for the program was procured from Southern Alberta Institute of Technology (SAIT), who has offered a full-time certificate program for years with great success.

Multiple factors are anticipated to contribute to maintaining consistent student enrollment. Currently, there are no other post-secondary programs in British Columbia offering credentials in remotely piloted aircraft systems (RPAS). The program targets a broad audience, including

recent high-school graduates and individuals seeking to upskill or reskill. Scheduling one cohort of 16 students each spring will reduce the potential impact of adverse weather conditions on program operations and enable effective delivery using existing faculty resources.

School of Construction & the Environment (SoC&E)
Diploma in Construction Management

The Diploma in Construction Management addresses a critical gap between existing certificate programs and the Bachelor of Technology in Construction Management. It provides a direct pathway for high school graduates, newcomers, and mid-career professionals to obtain formal education while remaining employed. Graduates will acquire essential skills to manage complex construction projects from planning through completion.

Industry demand for project managers, supervisors, and estimators supports the program's relevance. The flexible learning model enables students to gain practical experience concurrently, making it especially suitable for those transitioning from trades to management roles.

With three annual intakes of 24 students, this 75-credit diploma offers a structured entry and advancement route within the construction management field.

CERTIFICATE IN PROFESSIONAL REMOTELY PILOTED AIRCRAFT SYSTEMS

BUSINESS PLAN

EXECUTIVE SUMMARY
NEW PROGRAM PROPOSAL - BUSINESS PLAN
Certificate in Professional Remotely Piloted Aircraft Systems

Audit and Finance Committee (Business Plan): November 18, 2025
Board of Governors Meeting (Proposal & Business Plan): December 3, 2025

Notice of Intent	Final Proposal & Business Plan
Education Council reviewed: September 24, 2025	✓

1.	EXECUTIVE OVERVIEW OF PROPOSED PROGRAM	
a.	Proposed credential	Certificate in Professional Remotely Piloted Aircraft Systems
b.	Name of School	School of Transportation (SoT)
c.	Brief Program Description	
	The proposed Certificate in Professional Remotely Piloted Aircraft Systems is a 36-credit program that will be delivered in person during an 18-week period. The program will be delivered in a cohort format primarily at the Aerospace Technology Campus (ATC). The remotely piloted aircraft systems (RPAS) industry—commonly referred to as the drone industry— is a rapidly expanding sector that encompasses the design, manufacturing, operation, and maintenance of uncrewed aerial vehicles (UAVs) and their supporting systems. These aircraft are controlled remotely by certified pilots using sophisticated onboard sensors. RPAS are used in a wide range of applications, including aerial surveying, agricultural monitoring, infrastructure inspection, environmental assessment, public safety, and emergency response. The proposed program is designed to meet the growing demand for skilled professionals in the rapidly evolving field of drone technology. As industries such as agriculture, infrastructure, and environmental monitoring increasingly rely on remotely piloted aircraft systems (RPAS) for data collection, inspection, and mapping, the need for qualified operators and technicians has never been greater. Graduates of this program will expand their competencies or find employment opportunities in such occupations as Technical Occupations in Geomatics and Meteorology (NOC 22214), Aerospace Engineers (NOC 21390), Other Service Support Occupations (NOC 65329). The primary audience for the program includes individuals seeking to enter the RPAS field, including high school graduates and those looking to change their career or to expand their skill set in response to the growing drone industry. The proposed program aligns with BCIT's Strategic Plan (2025-2030) commitments by embracing digital transformation and advancing workforce readiness and regional economic development. The program also reflects BCIT's ongoing commitment to reconciliation and Indigenization by fostering meaningful engagement with Indigenous communities. Two seats per intake will be allocated specifically for Indigenous students to promote equitable access and representation.	
d.	Location of program [campus]	ATC Campus
e.	Delivery model	In-person
f.	Anticipated start date	Spring 2026
g.	Program duration	18 weeks
h.	Anticipated student enrolment [at steady state]	16 annually
i.	PAC/Industry support	Yes

2.	KEY ASSUMPTIONS	
a.	Potential students	The program targets a diverse range of students, including high school graduates, mid-career professionals, and individuals seeking to transition into the growing RPAS industry. The primary audience consists of those with little to no prior experience in RPAS, making it accessible to a wide demographic.
b.	Labour demand	The Canada Drone Market Size and Outlook for 2024-2030 shows that the demand for qualified and certified RPAS pilots in Canada is growing rapidly. With a compound annual growth rate of 16% between 2024 and 2030. According to the British Columbia Labour Market Outlook: 2024 Edition the combined demand for professions targeted by this program is 10,500 employees.

c.	Tuition determination	Posted tuition is $590 per week. Due to the amount of materials used, and advanced shop space and equipment we are adding a mandatory fee of $18 per week.
d.	Competitor analysis [i.e. the ones included in the NOI. Please list them in bullet points for easy comparison]	There are no other programs like this in BC. Selkirk College offers micro-credentials that are not directly comparable with the proposed program. Southern Alberta Institute of Technology (SAIT) offers a similar program, and further east Medicine Hat, Mohawk, and Nova Scotia Community College offer similar certificates.
e.	School capacity/faculty capacity	We have the classrooms, shop, equipment and faculty available.
f.	Other (Please Identify)	The program curriculum was obtained from SAIT, in a curriculum exchange. Additional costs will involve updates and contextualization of the curriculum for BC.

3.	**FINANCIAL HIGHLIGHTS**	
a.	Net Profit/Loss to BCIT at steady state	$18,836
b.	Source of funding	Tuition only
c.	Tuition determination	
i.	Program tuition	$590 weekly, plus $18/week mandatory fee = $10,944 for 18-week program
ii.	Provide benchmark comparison to similar programs [see 2d above]	Southern Alberta Institute of Technology charges $10,386 for 15-week program
d.	Capital costs [e.g. equipment, renovations, etc.]	None
e.	Direct Operating costs	Direct operating costs include faculty and support staff salaries

FINANCIAL SUMMARY	Steady State	Cumulative over 5 years
Tuition	$ 189,538	$ 845,146
Grant Funding (if applicable)	$ -	$ -
Total Revenue	$ 189,538	$ 845,146
One-time Startup Costs	$ -	$ 34,097
Direct Costs		
Faculty/support staff costs	$ 102,128	$ 491,001
Non Salary costs	$ 11,713	$ 48,841
Indirect Costs		
Overhead @ 30% of Revenue	$ 56,861	$ 253,544
Net Profit/(Loss)	**$ 18,836**	**$ 17,663**

4.	**IMPACTS TO KEY AREAS**	
a.	Facility Space Requirements [e.g. special dedicated space and/or renovations needed]	N/A
b.	Information Technology Services (ITS)	N/A
c.	Student Services	N/A

d.	Other [Please identify]	N/A

5. RISKS AND PROBABILITIES

A low risk would be if we cannot fill the classes, however this is mitigated by the higher weekly tuition rate. We believe it will take some time to spread the word and market this program. We also believe it could take time to build partnerships with industry who are looking for graduates of this program.
The curriculum was provided by SAIT and the program faculty will contextualize it for the BC enrollment and develop additional content relevant for BC.

APPROVALS

Provost and VP Academic
(Jennifer Figner)

Date: November 6, 2025

CFO and VP, Administration
(Navida Suleman)

Date: November 7, 2025

BUSINESS FORECAST

Part A - One-time Start Up Costs

INITIATIVE
Audit and Finance Committee (Business Plan): November 18, 2025

Projected Development and One-time Costs

Projected Development & One-time Costs

	Hours	Rates	Total	Comments
Development				
Salary				
Instructor/Faculty	400.0	$ 69.87	$ 27,949	**Note 1**
Support Staff			$ -	
Project Management			$ -	
Benefits			$ 6,149	**Note 2**
Total Salary Costs			**$ 34,097**	
Non Salary				
Materials, supplies, etc.			$ -	
Capital				
Renovations			$ -	
Equipment			$ -	
Total Non Salary Costs			**$ -**	
Total Development & One-time Costs			**$ 34,097**	

NOTES:

Note 1. Faculty adoption and expansion of the curriculum from SAIT, with focus on adapting curriculum to work with local Indigenous communities and providing training for faculty.

Note 2. The benefits are calculated at 22% FT

BUSINESS FORECAST

Part B - Course Delivery Forecast

INITIATIVE

Audit and Finance Committee (Business Plan): November 18, 2025

	Number of Sections				
Course Number	Year 1	Year 2	Year 3	Year 4	Year 5
Class #1	1				
Class #2		1			
Class #3			1		
Class #4				1	
Class #5					1
Class #6					
Class #7					
Class #8					
Class #9					
Class #10					
Class #11					
Class #12					
Class #13					
Class #14					
Class #15					
Class #16					
Totals					

			Revenue per Course				
# Credits	# Hours	Tuition/ course	Fiscal Yr1	Fiscal Yr2	Fiscal Yr3	Fiscal Yr4	Fiscal Yr5
36	540	10,944	10,944	11,163	11,386	11,614	11,846
36	540	$ 10,944	$ 10,944	$ 11,163	$ 11,386	$ 11,614	$ 11,846

	Year 1	Year 2	Year 3	Year 4	Year 5
Estimated number of students (total)	12	14	16	16	16
Number of sets	1	1	1	1	1
Capacity per set	16	16	16	16	16

Note: Tuition projected to increase by 2% per year

BUSINESS FORECAST

Part C - Financial Forecast

INITIATIVE
Audit and Finance Committee (Business Plan): November 18, 2025

FINANCIAL FORECAST	Year 1	Year 2	Year 3	Year 4	Year 5 Steady State	Cumulative Total	
Revenue							
Tuition and related fees	$ 131,328	$ 156,280	$ 182,178	$ 185,822	$ 189,538	$ 845,146	Note 1
Grant Funding (if applicable)						$ -	
Contract revenue - training/service	$ -	$ -	$ -	$ -	$ -	$ -	
Miscellaneous revenue (describe)	$ -	$ -	$ -	$ -	$ -	$ -	
Total Revenue	$ 131,328	$ 156,280	$ 182,178	$ 185,822	$ 189,538	$ 845,146	
Expenses							
Direct							
One-time Start up Costs							
Salary	$ 34,097	$ -	$ -	$ -	$ -	$ 34,097	Note 2
Non Salary	$ -	$ -	$ -	$ -	$ -	$ -	
Total One-time	*$ 34,097*	*$ -*	*$ -*	*$ -*	*$ -*	*$ 34,097*	
Academic and related Delivery costs							
Salary							
Instructor/Faculty	$ 64,336	$ 65,623	$ 66,935	$ 68,274	$ 69,639	$ 334,808	Note 3
Support Staff	$ 13,000	$ 13,260	$ 13,525	$ 13,796	$ 14,072	$ 67,653	
Department Head						$ -	
Benefits	$ 17,014	$ 17,354	$ 17,701	$ 18,055	$ 18,416	$ 88,541	Note 4
Total Salary	*$ 94,350*	*$ 96,237*	*$ 98,162*	*$ 100,125*	*$ 102,128*	*$ 491,001*	
Non-salary Expenses							
Materials/supplies	$ 8,000	$ 8,800	$ 9,680	$ 10,648	$ 11,713	$ 48,841	Note 5
Advertising/Marketing						$ -	
Other	$ -	$ -	$ -	$ -	$ -	$ -	
Lease costs	$ -	$ -	$ -	$ -	$ -	$ -	
Other (please list)	$ -	$ -	$ -	$ -	$ -	$ -	
Total Non-salary	*$ 8,000*	*$ 8,800*	*$ 9,680*	*$ 10,648*	*$ 11,713*	*$ 48,841*	
Total Direct	**$ 136,447**	**$ 105,037**	**$ 107,842**	**$ 110,773**	**$ 113,840**	**$ 573,940**	
Indirect							
Overhead @ 30% of Revenue	$ 39,398	$ 46,884	$ 54,653	$ 55,747	$ 56,861	$ 253,544	
Total Indirect	**$ 39,398**	**$ 46,884**	**$ 54,653**	**$ 55,747**	**$ 56,861**	**$ 253,544**	
Total Expenses *(Direct & Indirect)*	**$ 175,846**	**$ 151,921**	**$ 162,495**	**$ 166,520**	**$ 170,702**	**$ 827,484**	
NET Profit/(Loss)	**$ (44,518)**	**$ 4,359**	**$ 19,683**	**$ 19,302**	**$ 18,836**	**$ 17,663**	
NET Profit/(Loss) as a % of Net Revenues	**-34%**	**3%**	**11%**	**10%**	**10%**	**2%**	

Note 1: Added a $18 per week mandatory fee due to the nature of the work, shop supplies, and advanced shop equipment
Note 2: We obtained the curriculum from SAIT, it needs to be brought up to BCIT standards, and faculty need training.
Note 3: 18 week delievery, plus 2 weeks prep
Note 4: Benefits calculated at 22% (full time rate)
Note 5: Some general shop supplies may be needed, and software subscription. This is recovered via the $18/week fee.
Students buy their own drone kit

BUSINESS FORECAST
Key Assumptions

INITIATIVE

Audit and Finance Committee (Business Plan): November 18, 2025

5 Year Business Forecast: Key Assumptions

Comment on the following:

1 Revenue / cost sharing model (School/Institute; School/School; BCIT/External institutions)

Tuition only. Standard overhead included

2 Primary Sources of Revenue for program (tuition only, tuition + grant):

Tuition only, plus shop supply fee

3 Tuition assumptions and how determined (benchmark with similar programs at other institutions):

SAIT = $10,386 for 15 weeks at 35 hours/week (525 hours).
BCIT = $10.944 for 18 weeks at 30 hours/week (540 hours). We increased our program length by 15 hours or 3% compared to SAIT, based on SAIT feedback that the 525 hours is challenging for some students.

4 Primary categories of cost for the program:

Faculty and support costs are the primary costs of running this program
Some material/supply costs (consumables)

5 Identify any capital equipment costs required to launch program:

N/A, equipment already exists, and therefore we will increase the utilization of that equipment

6 Identify Faculty salary assumptions (new hire vs existing, full time vs part time contract, typically @ top-step rate unless otherwise known)

We would need 0.6 FTE faculty for the 18 week program

7 Identify significant ($10,000 +) impacts to other departments (e.g. facilities, IT, etc.) and action plan to implement:

With only 16 additional students per year the impact is minimal

DIPLOMA IN CONSTRUCTION MANAGEMENT

BUSINESS PLAN

EXECUTIVE SUMMARY
NEW PROGRAM PROPOSAL - BUSINESS PLAN
Diploma in Construction Management

Audit and Finance Committee (Business Plan): November 18, 2025
Board of Governors Meeting (Proposal & Business Plan): December 3, 2025

Notice of Intent	**Final Proposal & Business Plan**
Education Council reviewed: September 24, 2025	✓

1.	**EXECUTIVE OVERVIEW OF PROPOSED PROGRAM**		
	a.	Proposed credential	Diploma in Construction Management
	b.	Name of School	School of Construction and the Environment (SOCE)
	c.	Brief Program Description	
		The credential is a Diploma comprised of 75 credits. The program is designed in a flexible learning delivery model anticipated to be completed by most students in approximately 4 years (3-7 years). The delivery mode is flexible learning, course-by-course registration. The Diploma in Construction Management program aims to equip individuals with the knowledge and skills to effectively manage construction projects from pre-construction planning to project completion. Key areas of focus include project planning, cost control, scheduling, risk management, as well as legal, sustainable and ethical considerations within the construction industry. The target audience includes high school graduates, mid-career professionals, newcomers to Canada with construction experience, and graduates of related entry level BCIT Certificate programs in the construction field. It specifically includes students interested in pursuing the Bachelor of Technology in Construction Management by providing a flexible learning pathway. As noted above, another audience group includes new Canadian (or permanent residents) professionals who received training outside Canada and are enrolling in the program to leverage their background while gaining local knowledge and experience. The types of jobs graduates are prepared for, with the NOC codes and the expected job openings (2024-2034), include Construction Manager (NOC 70010) (10,220 job openings), Construction Supervisor (NOC 72014) (4,430 job openings) and Construction Estimator (NOC 22303) (1,490 job openings). This diploma is aligned with BCIT strategic plan initiatives (2025-2030): #4) Relevant Education and Sustainable practices and #11) Integrated Curriculum Development (with industry). The program has been developed using the IDEAS lens which is reflected in the fact that he program's advisory committee includes an Indigenous cultural consultant. In addition, the program will collaborate with the growing number of Indigenous owned and operated construction firms operating in the region to support the upskilling of their staff.	
	d.	Location of program	Burnaby campus
	e.	Delivery model	Online and In-Person (most courses available in both delivery models)
	f.	Anticipated start date	January-2026
	g.	Program duration	Flexible delivery (3-7 years)
	h.	Anticipated student enrolment	14
	i.	PAC/Industry support	The Diploma in Architectural Building Technology PAC's scope of advisory duties will expand to include this program. We have received confirmation of strong industry support, described in detail in the proposal for the new program.

2. KEY ASSUMPTIONS	
a. Potential students	A percentage of students graduating from the related four certificates will continue their studies in this program, and many will go on to ladder into the degree. Newcomers to BC with a background in construction will leverage this program to gain essential local knowledge upgrade. Students in this program will seek employment with, or be recruited by, construction firms and general contractors.
b. Labour demand	According to the British Columbia Labour Market Outlook: 2024 Edition the combined demand for professions targeted by this program is 16,140 employees. The deficit in Construction Managers, Supervisors and Estimators will continue as predicted and this program will help serve that need for industry. The flexible learning delivery mode will allow students to gain industry experience during their education. In addition, it is expected that a number of companies will sponsor their employees' education on a part-time basis while they gain industry experience and become embedded in their work teams (a long-term investment).
c. Tuition determination	This flexible delivery diploma is based on course-by-course registration into existing flexible learning courses. Tuition is $200/credit and increases by 2% annually.
d. Competitor analysis	Four similar programs exist in Canada and they are all **full-time**. The key elements of the curriculum are similar for all programs. **1. Southern Alberta Institute of Technology**, Calgary, AB, Civil Engineering Technology diploma, Construction Management Major (full-time, in-person) **2. George Brown College**, Toronto, ON, Construction Engineering Technician Program diploma (full-time, hybrid) **3. Mohawk College**, Hamilton, ON, Construction Engineering Technician (full-time, in-person) **4. Nova Scotia Community College**, Dartmouth, NS, Construction Project Management diploma (full-time, blended)
e. School capacity/faculty capacity	SOCE's Building Design and Construction Technology department has enough qualified flexible learning faculty to instruct the courses associated with the program.
f. Other (Please Identify)	All of the courses in the program, except 1, are already developed and running. This makes for an appealing business case, with so little upfront investment required.

3. FINANCIAL HIGHLIGHTS	
a. Net Profit/Loss to BCIT at steady state	$80,594
b. Source of funding	Course by course tuition
c. Tuition determination	
i. Program tuition	$15,000 ($200.00 x 75 credits)

		ii.	Provide benchmark comparison to similar programs [see 2d above]	See above 2d 1. Southern Alberta Institute of Technology- $15,883 2. George Brown College - $8,076 3. Mohawk College - $5,416 4. Nova Scotia Community College - $7,240
	d.		Capital costs [e.g. equipment, renovations, etc.]	No capital cost expenditures
	e.		Direct Operating costs	No additional direct operation costs

FINANCIAL SUMMARY	Steady State	Cumulative over 5 years
Tuition	$ 155,870	$ 582,339
Grant Funding (if applicable)	$ -	$ -
Total Revenue	$ 155,870	$ 582,339
One-time Startup Costs	$ -	$ 5,356
Direct Costs		
Faculty/support staff costs	$ 28,515	$ 137,092
Non Salary costs	$ -	$ -
Indirect Costs		
Overhead @ 30% of Revenue	$ 46,761	$ 174,702
Net Profit/(Loss)	**$ 80,594**	**$ 265,189**

4.	IMPACTS TO KEY AREAS	
a.	Facility Space Requirements [e.g. special dedicated space and/or renovations needed]	No significant impact to Facilities. Existing classrooms will be used to deliver the program. No upgrades or renovations required.
b.	Information Technology Services (ITS)	No significant impact to ITS resources. Existing ITS staff and infrastructure will support the program.
c.	Student Services	Program Advising, Financial Aid and International.
d.	Other [Please identify]	No other.

5.	RISKS AND PROBABILITIES

Currently, BCIT is the only post-secondary institution to offer construction management programming for the province. Not having a flexible learning option is a gap in the way we serve this growing industry. With an extensive existing catalogue of related courses, our existing collection of entry-level feeder programs, and our close relationship with BC's construction industry, BCIT is uniquely positioned to offer this program.

The creation and provision of this program represents one of BCIT's core operating mandates in that it responds to the current and future challenges for the training and supply of skilled labour in the construction industry. BCIT's unique relationship with a wide range of construction industry partners makes the Institute's role in meeting this need for industry a natural fit.

There is a risk in not offering this program now in that another enterprising post-secondary entity might identify the opportunity and fast-track its development. BCIT would also miss out on the opportunity to expand the offering of a flexible training option for young people starting their careers, or mid-career professionals who are considering a career field change. Potential employers will also gain a pathway for training their employees.

There is a theoretical risk in offering this program and it not having sufficient enrolments. As unlikely as this is, for the many reasons mentioned throughout, the business case for this program is appealing partly because there will be little need for course development as this is primarily restructuring existing construction management-related courses into a more cohesive pathway. Furthermore, since all but one of the courses in this program are already offered in related programs, the proposed program is expected to increase enrollment in existing courses.

APPROVALS

Provost & VP Academic
(Jennifer Pigner)

Date: November 6, 2025

CFO and VP, Administration
(Navida Suleman)

Date: November 7, 2025

BUSINESS PLAN

Part A - One-time Start Up Costs

INITIATIVE
Diploma in Construction Management

Projected Development and One-time Costs

Projected Development & One-time Costs	Hours	Rates	Total		Comments	
Development						
Salary						
Instructor/Faculty	72.0	$ 60.98	$ 4,391		**Note 1**	
Support Staff			$ -			
Project Management			$ -			
Benefits			$ 966			
Total Salary Costs			**$ 5,356**			
Non Salary						
Materials, supplies, etc.			$ -			
Capital						
Renovations			$ -			
Equipment			$ -			
Total Non Salary Costs			**$ -**			
Total Development & One-time Costs			**$ 5,356**			

NOTES:

Note 1: Development of one 6-credit close-out course drawing from existing material and repackaging (not a lot of research or writing). The course will be developed in year 1, but it is the last course that students will take in the program.

BUSINESS PLAN

Part B - Course Delivery Plan

INITIATIVE

Diploma in Construction Management

Term Number	Number of Sections Year 1	Year 2	Year 3	Year 4	Year 5
Term 1 (See Note: 1)	1	1	1	1	1
Term 2	1	1	1	1	1
Term 3	1	1	1	1	1
Totals					

# Credits	# Hours	Tuition/term	Tuition Fiscal Yr1	Fiscal Yr2	Fiscal Yr3	Fiscal Yr4	Fiscal Yr5
6	72	1,200	14,400	29,376	47,442	50,938	51,957
6	72	1,200	14,400	29,376	47,442	50,938	51,957
6	72	1,200	14,400	29,376	47,442	50,938	51,957
18	216	$ 3,600	$ 43,200	$ 88,128	$ 142,327	$ 152,814	$ 155,870

	Year 1	Year 2	Year 3	Year 4	Year 5
Estimated number of students (total)	12	24	38	40	40
Number of sets (See Note: 3)	1	1	1	1	1
Capacity per set	N/A	N/A	N/A	N/A	N/A

NOTES:

Note 1: We are doing this by term rather than by course because this is course-by-course registration, not cohort, and not all students in each course will be in this program. We assume some students will graduate after year 3.

Note 2: We are assuming the average student in this program will take 6 courses per year/2 per term (6 credits per term).

Note 3: For the purpose of calculation we include 1 set, however, in the flexible learning mode students will not be taking courses in a cohort format. Since there are no sets the capacity per set is not relevant

BUSINESS PLAN
Part C - Financial Plan

INITIATIVE
Diploma in Construction Management

FINANCIAL PLAN	Year 1	Year 2	Year 3	Year 4	Year 5 Steady State	Cumulative Total	
Revenue							
Tuition and related fees	$ 43,200	$ 88,128	$ 142,327	$ 152,814	$ 155,870	$ 582,339	**Note 1**
Grant Funding (if applicable)	$ -	$ -	$ -	$ -	$ -	$ -	
Contract revenue - training/service	$ -	$ -	$ -	$ -	$ -	$ -	
Miscellaneous revenue (describe)	$ -	$ -	$ -	$ -	$ -	$ -	
Total Revenue	$ 43,200	$ 88,128	$ 142,327	$ 152,814	$ 155,870	$ 582,339	
Expenses							
Direct							
One-time Start up Costs							
Salary	$ 5,356	$ -	$ -	$ -	$ -	$ 5,356	**Note 2**
Non Salary	$ -	$ -	$ -	$ -	$ -	$ -	
Total One-time	*$ 5,356*	*$ -*	*$ -*	*$ -*	*$ -*	*$ 5,356*	
Academic and related Delivery costs							
Salary							
Instructor/Faculty	$ 26,343	$ 26,870	$ 27,408	$ 27,956	$ 28,515	$ 137,092	**Note 2**
Support Staff	$ -	$ -	$ -	$ -	$ -	$ -	**Note 3**
Program Head	$ -	$ -	$ -	$ -	$ -	$ -	**Note 3**
Benefits	$ -	$ -	$ -	$ -	$ -	$ -	
Total Salary	*$ 26,343*	*$ 26,870*	*$ 27,408*	*$ 27,956*	*$ 28,515*	*$ 137,092*	
Non-salary Expenses							**Note 4**
Materials/supplies	$ -	$ -	$ -	$ -	$ -	$ -	
Advertising/Marketing	$ -	$ -	$ -	$ -	$ -	$ -	
Other	$ -	$ -	$ -	$ -	$ -	$ -	
Lease costs	$ -	$ -	$ -	$ -	$ -	$ -	
Other (please list)	$ -	$ -	$ -	$ -	$ -	$ -	
Total Non-salary	*$ -*	*$ -*	*$ -*	*$ -*	*$ -*	*$ -*	
Total Direct	**$ 31,700**	**$ 26,870**	**$ 27,408**	**$ 27,956**	**$ 28,515**	**$ 142,448**	
Indirect							
Overhead @ 30% of Revenue	$ 12,960	$ 26,438	$ 42,698	$ 45,844	$ 46,761	$ 174,702	
Total Indirect	**$ 12,960**	**$ 26,438**	**$ 42,698**	**$ 45,844**	**$ 46,761**	**$ 174,702**	
Total Expenses *(Direct & Indirect)*	**$ 44,660**	**$ 53,309**	**$ 70,106**	**$ 73,800**	**$ 75,276**	**$ 317,150**	
NET Profit/(Loss)	**$ (1,460)**	**$ 34,819**	**$ 72,221**	**$ 79,014**	**$ 80,594**	**$ 265,189**	
NET Profit/(Loss) as a % of Net Revenues	**-3%**	**40%**	**51%**	**52%**	**52%**	**46%**	

NOTES

Note 1: 6 courses per year per student ($200/credit)

Note 2: The only costs associated with it are instructional costs and the development of 1 close-out course. Other courses for this diploma are already in existance and being taught as part of other programs, hence no incremental costs.

Note 3: This program will be managed by an existing related program head.

Note 4: There are no non-usable in this program because all courses aredelivered online.

BUSINESS PLAN
Key Assumptions

INITIATIVE

Diploma in Construction Management

5 Year Business Plan: Key Assumptions

Comment on the following:

1 Revenue / cost sharing model (School/Institute; School/School; BCIT/External institutions)

None

2 Primary Sources of Revenue for program (tuition only, tuition + grant):

Tuition only

3 Tuition assumptions and how determined (benchmark with similar programs at other institutions):

$200 x 75 credits = $15,000. The verage tuition for all existing courses that will be offered as part of this program is $200.

The overall cost is similar to SAIT and more expensive than the other three educational institutions. Considering BCIT's brand, and it being the only program in BC, and being the only felxible learning program, we are confident in its appeal over competitor programs.

4 Primary categories of cost for the program:

Instructional fees calculated at $121.96/hr and increasing by 2% year over year (no benefits included).
Start-up includes development of 1 course.

5 Identify any capital equipment costs required to launch program, and to sustain the program:

None

6 Identify Faculty salary assumptions (new hire vs existing, full time vs part time contract, typically @ top-step rate unless otherwise known)

Part-time faculty will be teaching these courses (assumed at top-step).

7 Identify significant ($10,000 +) impacts to other departments (e.g. facilities, IT, etc.) and action plan to implement:

None

Board of Governors Open Meeting – December 3, 2025

8.0 Next Meeting and Conclusion

- February 24, 2026 at 1:00 p.m.