Information Security

Policy No:	3502
Version:	3
Category:	Information Management
Approving Body:	Board of Governors
Executive Sponsor:	Chief Information Officer
Department Responsible:	Information Technology Services
Directory of Records Class:	0650-15
Approval Date:	2020 MAY 26

Policy Statement

BCIT will take appropriate measures to preserve and secure the confidentiality, integrity, and availability of all information in its custody and or under its control, including all data stored in and transmitted through BCIT computing, communications, networking, and other information technology resources, and including all data recorded in print 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.

Purpose of Policy

The purpose of this policy is to:

- 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 connect to BCIT information assets.

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.

[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

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.

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.

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.

b) 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.

10. Consequences of Policy Violation

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 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.

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

Scheduled Review Date

2025 May 26