



Information Security

Policy No.:	3502
Category:	Information Technology Services
Approving Body:	Board of Governors
Executive Division:	Learning and Technology Services
Department Responsible:	Information Technology Services
Current Approved Date:	2009 Jan 27

Policy Statement

BCIT is committed to taking appropriate measures to preserve the confidentiality, integrity, and availability of information and information technology (IT). This policy applies to all BCIT information and computing, communications, and networking resources connected to Institute facilities and the users of these resources.

Purpose of This Policy

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

The purpose of this policy is to:

- Protect the confidentiality, integrity, and availability of BCIT information and associated information technology
- Provide management direction and support for information security in accordance with business requirements and relevant laws and regulations
- 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.

Table of Contents

Policy Statement	1
Purpose of This Policy	1
Application of This Policy	2
Related Documents and Legislation	2
Definitions	3
Guiding Principles	7
Duties and Responsibilities	8
1. Organization of Information Security	8
2. Asset Management	11
3. Human Resources Security	13
4. Physical and Environmental Security	14
5. Communications and Operations Management	16
6. Access Control	22
7. Information Systems Acquisition, Development & Maintenance	24
8. Information Security Incident Management	25
9. Business Continuity Management	26
10. Compliance	26
11. Non-Conforming Systems	27
12. Consequences of Policy Violation	27
Procedures and Guidelines Associated With This Policy	27
Forms Associated With This Policy	27
Special Situations	27
Amendment History	28
Scheduled Review Date	28

Application of This Policy

This policy applies to everyone who uses BCIT information technology assets, including those who use their own personal equipment to connect to BCIT information assets.

Related Documents and Legislation

BCIT Policies:

1504, Standards of Conduct and Conflict of Interest
 3501, Acceptable Use of Information Technology
 5102, Standards of Non-academic Conduct
 6601, Intellectual Property
 6700, Freedom of Information and Protection of Privacy (FOIPOP)
 6701, Records Management
 7506, Copyright Compliance
 7525, Protection of Equipment, Property and Information
 7530, Emergency Response

Legislation applicable to this policy includes:

- *BC College and Institute Act*
- *BC Freedom Of Information and Protection of Privacy (FOIPOP) Act*
- *BC Personal Information Protection (PIP) Act*
- *The Criminal Code of Canada*
- *Canada Copyright Act.*

Definitions

Account: establishes a relationship between a user and a set of information assets. By logging in to an account, the user is authorized to perform a specified set of actions against a corresponding set of information assets for the time the user remains authenticated to the account (for that login session).

Asset: anything that has value to the Institute.

Asset Custodian: the BCIT employee responsible for locating a physical information asset (i.e. equipment) upon request. All information assets must have an assigned custodian.

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

Authorized User: a user who is authorized to perform the specified action on an asset. Part of the authorization process may require that the person exhibit the necessary qualifications to perform the action.

BCIT Internal Use: as defined in section 2.2 Information Classification.

Business Continuity: 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 7530, Emergency Response for more information.

Confidential Information: as defined in section 2.2 Information Classification.

Control: a means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature. Note: Control is also used as a synonym for safeguard or countermeasure.

Data: items representing facts that consist of text, numbers or images and stored in electronic information systems. Data are the raw materials that are processed or interpreted to create information. Institute data is all data related to, received by, or created by BCIT.

Denial of Service: actions that intentionally prevent any Information Processing Facility from functioning in accordance with its intended purpose

Disaster Recovery: refers to the activities that restore the Institute to an acceptable condition after suffering a disaster. See Policy 7530, Emergency Response for more information.

Encryption: the process of obscuring information to make it unreadable without special knowledge (i.e., "scrambling" the information). That special knowledge is often a "key" that is used to decrypt the information so it can be read. Conceptually, the key is similar to a password that provides access to the encrypted information.

Equipment: information technology equipment.

External Party: an organization or an individual who is not an employee or student who requires access to BCIT's information assets, excluding public assets.

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

Inactive Account: an account that has remained unused for the period of time specified in Guideline 3502, Information Security.

Information: includes all forms of data, documents, records, communications, conversations, messages, recordings, and photographs. It includes everything from digital data and email to faxes and telephone conversations.

Information Asset: an asset that is comprised of information or of equipment or systems for the processing of information.

Information Owner: the BCIT employee who classifies the specified information.

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

Information Security: 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 Framework: a comprehensive approach to preserve information security including:

- Organizational structures with clearly defined roles and responsibilities
- Risk assessment and impact analysis
- Guiding principles
- Policies, guidelines, and procedures
- 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: an identified occurrence of a system, service, or network state indicating a possible or pending breach of information security or breach of acceptable use or failure of safeguards or a previously unknown situation that may be security relevant.

Information Security Officer: oversees the Institute's Information Security program. This includes providing leadership and guidance in information security and information risk management, developing information security policies and guidelines, and overseeing the information security incident response team.

IT Administrator: the person responsible for configuring access to and monitoring access, usage, and performance of an information asset, including system administrator, network administrator, application administrator, and database administrator (DBA).

Least Privilege: the principle that requires each user to be granted the most restrictive set of privileges needed for the performance of authorized tasks.

Login Session: a period between a user logging in and logging out of an account.

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

Media: includes removable media and fixed storage devices.

Mobile Device: any electronic device that is portable and contains or has the ability to contain information or provides the ability to access or transmit Personal or Confidential information. Examples include laptop, tablet PC, PDA, RIM BlackBerry, and Palm Treo.

Network Equipment: 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, DHCP, WINS, and DNS servers.

Network Zone: Different networks, and often different segments of a given network, have diverse security characteristics and requirements. For security, each network must be divided into one or more logical network zones. Each network zone is a logically connected part of the network, whose security is managed in a coherent fashion.

Defined zones include:

- Administrative Zone – for key business users and systems
- Academic Zone – for faculty and students for the purposes of teaching
- Residence Zone – for students in residence
- DMZ – for systems connected to the Internet or other outside network.

Password: the sequence of characters and numbers used to authenticate a user's identity, which is known only to that user.

Personal Information: as defined in section 2.2 Information Classification.

Public Assets: designated BCIT information assets that are available to members of the public with authorization required. Examples include kiosks and the public website.

Public Information: as defined in section 2.2 Information Classification.

Record: See Policy 6701, Records Management for definition of a record.

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

Server: a computer whose function is to provide services (e.g., access to files, printing, and shared applications including websites; database management; communications; and access to Personal or Confidential information) on which end users depend on an ongoing basis. Computers that are used to provide network services such as DHCP, DNS, and LDAP are considered to be network equipment and are not servers for the purpose of this policy.

Student Server: a computer set up by faculty or students as part of a course to teach server technology and principles.

System: a collection of components including hardware and software designed to store, process, or transmit information in support of a business outcome.

System Owner: the BCIT employee responsible for a given system.

Threat: a potential cause of an unwanted incident, which may result in harm to a system or organization.

User: a person who performs any action on an information asset.

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

Guiding Principles

1. By nature, a post secondary education institute needs to share information for the purpose of delivering education. Security measures must be implemented in a manner that enables appropriate information exchange.
2. Security responsibilities and accountability must be clearly defined and acknowledged.
3. Users are personally accountable for the protection of information assets under their control and must take appropriate measures to protect the confidentiality, integrity, and availability of the assets.
4. Users should have sufficient training to allow them to properly protect information assets.
5. Security controls must be cost-effective and in proportion to the risks and the value of the assets that need to be protected.
6. Security is multi-disciplinary and requires a comprehensive and integrated approach covering every aspect of BCIT's operations.
7. All parties should act in a timely, coordinated manner to prevent and respond to security incidents.
8. Security must be periodically assessed to ensure that adequate measures are in place to protect the assets of BCIT.
9. Permissions are assigned so that the least amount of privilege required to fulfill the business function is given (least privilege).
10. No single mechanism may protect an asset from unknown threats. Where warranted, multiple layers of controls should be employed to reduce the risk of failure of any single measure (defence in depth).
11. Compromise of one asset should not lead to the further compromise of other assets (compartmentalization).
12. Many information systems have not been designed with security in mind. Where adequate security cannot be achieved through technical means, alternate controls must be implemented.

Duties and Responsibilities

1. Organization of Information Security

1.1 Internal Organization

1.1.1 *Management Commitment to Information Security*

The Board of Governors and BCIT Executive actively support information security within the organization.

1.1.2 *Allocation of Information Security Responsibilities*

Board of Governors

The BCIT Board of Governors is accountable for the establishment of 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 framework, including periodic, independent reviews.

Information Security Officer

The Information Security Officer is responsible for:

- Recommending an appropriate Information Security Framework to the BCIT Executive
- Providing day-to-day monitoring of the framework
- Informing the BCIT Executive of security risks and management plans
- Establishing appropriate contacts with security forums, professional associations, and other groups with specialist interests in information security.

BCIT Management

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

Instructors and Teaching Faculty

Instructors and Teaching Faculty are responsible for ensuring that students under their supervision are aware of their information security responsibilities.

Information Owners

Information Owners are responsible for classifying information in accordance with policies and guidelines. (See Guideline 3502, Information Security and Procedure 3502, Information Security for details.) All information must have an assigned information owner.

System Owners

System owners are accountable for ensuring that systems are assessed for security requirements including those flowing from legislative and contractual obligations. System owners are also accountable for ensuring that systems are designed, configured, implemented, operated, maintained, upgraded, and decommissioned consistent with the established security needs.

Duties and Responsibilities

All systems must have an assigned system owner. System owners must ensure an IT administrator is assigned to each asset comprising the system. (See Procedure 3502, Information Security for details.)

Asset Custodians

Asset custodians, upon request, must be able to determine the location of information assets under their custodianship and must ensure that assets transferred from their custodianship are clearly assigned to the next custodian. All physical assets such as information technology equipment must have an assigned custodian. (See Procedure 3502, Information Security for details.)

IT Administrators

IT Administrators are responsible for configuring the security features of the assets under their administration in accordance with policy, guidelines, and other requirements. All assets with configurable security characteristics must have an assigned IT Administrator. (See Procedure 3502, Information Security for details.)

Information Technology Services

As the central provider of Information Technology, the ITS Department is responsible for:

- Network management and operation including the establishment of network zones and compartmentalization
- Delegation of administration of a network zone only when appropriate controls are in place in the delegated organization
- Maintaining a catalogue of core services including clearly articulated service level expectations
- Continuity of core enterprise class IT infrastructure as part of the Institute's overall business continuity framework.

Safety and Security Department

The Safety and Security Department is responsible for:

- The physical security of BCIT facilities including access control to buildings and rooms
- Overall emergency response, disaster planning, and business continuity planning
- Contact with authorities.

Marketing and Communications Department

The Marketing and Communications Department is responsible for:

- Protection of BCIT's brand from information security threats
- Communications with the media in the event of an information security incident
- Policies and procedures for use of BCIT domain names.

Human Resources

The Human Resources Department is responsible for:

- Documenting information security requirements in job descriptions
- Screening of employees
- Coordinating the termination of employees, ensuring all

Duties and Responsibilities

departments are appropriately notified.

Records Management Office

The Records Management Office is responsible for:

- Ensuring that the Directory of Records accurately reflects the classification of records
- Exchange agreements that involve the exchange of Personal information.

Financial Services Department

The Financial Services Department is responsible for ensuring controls are in place to protect the security of financial information and, in particular, to ensure the integrity of financial information.

Risk Manager

The Risk Manager is responsible for identifying and assessing overall risk for BCIT.

Users

All users are responsible for:

- Taking appropriate measures to prevent loss, damage, abuse, or unauthorized access to information assets under their control
- Promptly reporting all acts that may constitute real or suspected breaches of security including, but not limited to, unauthorized access, theft, system or network intrusions, willful damage, and fraud
- Looking after any physical device (tools, computers, vehicles, etc.) and access articles (keys, ID cards, system IDs, passwords, etc.) assigned to them for the purposes of performing their job duties, taking courses, conducting research, or otherwise participating within the Institute
- Respecting the classification of information as established by the information owner
- Complying with all the security requirements defined in this document
- Complying with other related policies including Policy 3501, Acceptable Use of Information Technology.

1.2 External Parties

1.2.1 *Identification of Risks Related to External Parties or Students*

The risks to the Institute's information assets relating to external parties or students must be identified and appropriate controls implemented before granting access.

1.2.2 *Addressing Security in External Party Agreements*

Access to BCIT information assets, except public assets, must not be granted to external parties without a contractual agreement that binds them to BCIT policies.

Duties and Responsibilities

2. Asset Management

2.1 Responsibility for Assets

Each piece of equipment must have an assigned asset custodian. Upon request asset custodians must be able to locate the equipment assigned to them. If custodians are to pass the custody of the equipment to another person, they are responsible for ensuring the record of custodianship is updated. If a custodian becomes unavailable unexpectedly, this responsibility falls to the operations manager of their department or school.

2.1.1 *Inventory of Assets*

An inventory of assets must be maintained.

2.1.2 *Acceptable Use of Assets*

See Policy 3501, Acceptable Use of Information Technology.

2.2 Information Classification

2.2.1 *Information Ownership*

All information must have a designated information owner. For complete information about establishing information ownership, see Guideline 3502, Information Security.

2.2.2 *Classifying Information*

All Institute information must be classified according to its requirements for confidentiality, integrity, and availability. The information owner is responsible for classifying the information according to Guideline 3502, Information Security.

Classification must be reviewed on a regular basis.

2.2.3 *Confidentiality Classifications*

The following confidentiality classifications determine how Institute information must be shared, handled and stored:

- **Public** – information that is available to the general public and is routinely disclosed
- **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
- **Confidential** – information that contains sensitive Institute information and that is available to authorized users. A formal FOIPOP request is required for non-routine disclosure
- **Personal** – information that contains sensitive personal information and is available to authorized users only. A formal FOIPOP request is required for non-routine disclosure.

2.2.4 *Business Continuity Classifications*

In addition to the confidentiality classifications, Policy 7530, Emergency Response governs the classification of information for business continuity purposes. Each information owner must classify information for the purposes of business continuity.

Duties and Responsibilities

2.2.5 Labelling Information

Both hard copy and electronic information must be clearly labelled with its confidentiality classification so that authorized users are aware of the classification. For complete details on how to label information, see Guideline 3502, Information Security.

2.3 Information Handling

Authorized users must carry out all tasks related to the creation, storage, maintenance, cataloguing, use, dissemination, and disposal of Institute information responsibly, in a timely manner, and with the utmost care. Users must not knowingly falsify information or reproduce information that should not be reproduced.

2.3.1 Sharing Institute Information

Personal, Confidential, and BCIT Internal Use information may only be shared with other authorized users, on a need to know basis.

2.3.2 Storing Information

Information classified as Personal or Confidential must be encrypted and stored with access limited to authorized users.

Secure storage of Institute information is a joint responsibility of system owners, IT administrators, database designers, application designers, and the information owner.

2.3.3 Printing of Personal or Confidential Information

Information classified as Personal or Confidential must never be sent to a shared printer without an authorized user immediately present to retrieve it and hence safeguard its confidentiality during and after printing.

2.3.4 Collection and Use of Personal Information

The collection, use, storage, and transmission of Personal information using BCIT information technology resources must be in compliance with the *B.C. Freedom of Information and Protection of Privacy Act* and with Policy 6700, Freedom of Information and Protection of Privacy.

2.3.5 Deleting Information Created or Owned by Others

Information is to be protected against unauthorized or accidental changes, and may only be deleted in accordance with procedures established by the information owner and in accordance with records management procedures.

Duties and Responsibilities

3. Human Resources Security

3.1 Prior to Employment

3.1.1 *Roles and Responsibilities*

Security roles and responsibilities of employees must be defined and documented in job descriptions.

3.1.2 *Screening*

Background verification checks on all candidates for employment, and external parties must be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

3.1.3 *Terms and Conditions of Employment*

All employees must acknowledge their agreement to abide by Policy 3501 and Policy 3502 prior to receiving access to any account. See Procedure 3502, Information Security.

3.2 During Employment

3.2.1 *Information Security Awareness, Education, and Training*

All employees and external parties, where applicable, must receive appropriate awareness training and regular updates in policies and procedures. New employees must receive security training as part of their initial orientation.

3.2.2 *Change of Role*

Change of responsibilities must be managed as a termination of the respective responsibilities and the assignment of new responsibilities as described in section 3.1 Prior to Employment.

3.3 Termination of Employment

3.3.1 *Termination Responsibilities*

An employee's continuing obligations to information security must be communicated in writing at termination of employment.

3.3.2 *Return of Assets*

All employees and external parties must return all of the Institute's assets in their possession upon termination of employment, contract, or agreement. The asset custodian is responsible to ensure the corresponding asset inventories are updated.

3.3.3 *Removal of Access Rights*

On leaving employment, all employee-based access must be disabled at the end of the employee's last day, or sooner, based on security requirements.

Duties and Responsibilities

4. Physical and Environmental Security

4.1 Secure Areas

4.1.1 *Physical Security Perimeter*

Security perimeters with well defined access points (barriers such as wall, card controlled entry) must be used to protect areas that contain Personal, Confidential, or BCIT Internal Use information and information processing facilities. Protection provided must be commensurate with identified risks. Mobile devices and removable media are excluded provided the information is encrypted as per section 5.7.2 Encryption of Information on Removable Media.

4.1.2 *Physical Entry Controls*

Areas requiring higher levels of security must be protected with appropriate entry controls to ensure that only authorized users are allowed access.

4.2 Equipment Security

4.2.1 *Equipment Siting and Protection*

The sites chosen to locate equipment or store information must be suitably protected from physical intrusion, temperature fluctuations, theft, fire, flood, and other hazards.

4.2.2 *Physical Security of Equipment*

Asset custodians are accountable (either directly or by delegation of responsibility) to ensure the physical security of assigned equipment regardless of whether the equipment is located on or off BCIT campuses.

4.2.3 *Mobile Devices*

BCIT owned mobile devices must be issued only to authorized users. They are to be used only by authorized users and only for the purpose for which they are issued. The information stored on the mobile equipment is to be suitably protected from unauthorized access at all times. See Procedure 3502, Information Security.

When using mobile devices, encryption standards must be followed. See also section 2.3 Information Handling.

4.2.4 *Use of Equipment On-Campus*

With the exception of public assets, only authorized users are permitted to use BCIT equipment.

4.2.5 *Supporting Utilities*

Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.

4.2.6 *Cabling Security*

Cabling carrying information or supporting information services must be protected from interception or damage. Power and cooling lines must be protected from damage.

Duties and Responsibilities

4.2.7 *Equipment Maintenance*

Equipment must be correctly maintained to ensure its continued availability and integrity.

4.2.8 *Security of Equipment Off-Campus*

Only authorized users are permitted to take non-mobile BCIT technology equipment off campus. When non-mobile BCIT equipment is used off campus, the authorized user is responsible for notifying the asset custodian and ensuring the security of the equipment at all times.

4.2.9 *Secure Disposal or Re-use of Equipment*

Equipment owned or leased by the Institute may only be disposed of or reconditioned for reuse by persons authorized to dispose of or recondition equipment who have ensured that the relevant security risks have been mitigated and all information has been rendered unrecoverable.

Duties and Responsibilities

5. Communications and Operations Management

5.1 Operational Procedures and Responsibilities

5.1.1 *Documented Operating Procedures*

Operating procedures must be documented, maintained, and made available to all users who need them.

5.1.2 *Change Management*

Changes to information processing facilities and systems must be controlled through appropriate change control mechanisms.

5.1.3 *Segregation of Duties*

Duties and areas of responsibility must be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Institute's assets.

5.1.4 *Separation of Development, Test, and Operational Facilities*

Development, test, and operational facilities must be separated to reduce the risks of unauthorized access or change to the operational system.

5.2 External Party Service Delivery Management

BCIT security requirements must be incorporated into contractual relationships with external parties. Compliance to security requirements must be monitored on an ongoing basis.

5.3 System Planning and Acceptance

Acceptance criteria for new information systems, upgrades, and new versions must be established and suitable tests of the system(s) carried out during development and prior to acceptance.

5.4 Protection against Malicious Code

Risks from malicious code to the Institute's systems and information must be minimized by fostering employee awareness, encouraging employee vigilance, and deploying appropriate protective systems and devices.

IT administrators must inform relevant parties of threats and countermeasures they can take to protect the Institute's systems and information. Users must stay informed about threats and take reasonable precautions in using Institute IT resources in order to minimize opportunities for attacks.

IT administrators must prepare and maintain contingency plans for a denial of service attack and periodically test their plans to ensure adequacy.

5.4.1 *Defending against Malicious Attack*

System hardware, operating system and application software, networks, and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

5.4.2 *Downloading Files and Information from the Internet*

Duties and Responsibilities

Users are responsible for all information and files they download from the Internet (or other external networks or from one network zone to another) and must safeguard against both malicious code and inappropriate material. See also Guideline 3502, Information Security.

5.4.3 Receiving Electronic Mail (Email)

Users must treat incoming email with the utmost care due to its inherent information security risks. The opening of files or other attachments that are from an unknown source is not permitted unless the user first scans the attachments for possible viruses or other malicious code. See Guideline 3501, Acceptable Use of Information Technology.

5.5 Backup

System owners are responsible for establishing the extent, frequency, and retention of system backups which must reflect 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. See also Guideline 3502, Information Security.

IT administrators are responsible for configuring information assets to meet backup requirements.

5.5.1 Backups must be Secured and Tested

Backups must be secured in accordance with the classification of the information they contain. Backups must be periodically tested to ensure the data is recoverable, and records must be kept of the tests.

5.5.2 Backups must not be Used in Lieu of Other Controls

BCIT backup facilities are not intended to replace records management controls or provide audit trails.

5.5.3 Recovering and Restoring Information

Safeguards must be in place to protect the integrity of data files when recovering and restoring data files, especially where restored files may replace more recent files.

5.6 Network Security Management

Networks must be adequately managed and controlled in order to be protected from threats and to maintain security for the systems and applications using the networks, including information in transit.

All equipment connected to the network is subject to all BCIT policies. Personal equipment that will be connected to the network may also be subject to inspection prior to connection in order to verify that security requirements are met.

5.6.1 Network Controls

Special controls must be established to:

- Safeguard the confidentiality and integrity of data passing over public networks or over wireless networks
- Protect network equipment, the connected systems, and

Duties and Responsibilities

- applications
- Maintain the availability of the network services and computers connected
- Apply appropriate logging and monitoring to enable recording of security relevant actions.

5.6.2 User Authentication for External Connections

Remote access control procedures must provide adequate safeguards through robust identification, authentication, and encryption techniques. Remote access to BCIT networks is only through the technology approved by the Information Security Officer. See Procedure 3502, Information Security.

5.6.3 Remote Configuration and Diagnostic Port Protection

Physical and logical access to configuration and diagnostic ports must be controlled.

5.6.4 Segregation in Networks – Network Zones

Each network zone must:

- Have clear guidelines as to the intended use of the zone and its security characteristics
- Be sufficiently secure for intended uses
- Be compartmentalized so as not to be a means for intrusion into, or interference with, BCIT systems or other networks
- Have redundancy, backup and recovery measures, and contingency plans in place to ensure that network services are available on a sufficiently timely basis to support the intended uses
- Have documentation covering its topology, configuration, and gateways to external networks and nodes, as well as the connected devices and individuals responsible.

Equipment, other than approved network equipment, must not be attached to two network zones simultaneously. This is to prevent uncontrolled flow of traffic between zones and to preserve compartmentalization.

5.6.5 Network Connection Control

Network equipment must not be connected to BCIT networks without approval from IT Services. See Procedure 3502, Information Security.

Systems and equipment connected to the BCIT network must be configured to minimize the possibility of bypassing access controls. IT administrators are responsible for implementing such precautions. See Guideline 3502, Information Security for configuration details.

5.6.6 IP Address Assignment

IP addresses on BCIT networks must not be assigned or used without permission from IT Services. (Automated assignment of an IP address by an ITS controlled DHCP server constitutes permission.)

5.6.7 Domain Name Registration and Use

Employees and students are not permitted to register domain names that

Duties and Responsibilities

include BCIT, British Columbia Institute of Technology, or any variations without prior authorization of the Marketing and Communications Department.

Third party agreement language must include protection for BCIT domain names. See section 1.2.2 Addressing Security in External Party Agreements.

All websites that are sub-domains of a BCIT domain or assigned to a BCIT owned IP range must be authorized by the Marketing and Communications Department prior to development.

5.6.8 Server Placement in Networks

Servers that are connected to the BCIT network must be placed in a location and network zone that is logically and physically secure commensurate with the value of the service provided and the sensitivity of the information accessible through the system. All access to this equipment must be logged to facilitate auditing. See Guideline 3502, Information Security for minimum logging standards.

Student servers may only be attached to the Academic Zone and must not be attached to the Administrative Zone.

5.6.9 Servers Accessible from External Networks

All servers that are accessible to an external network (including the Internet) must receive permission from the ISO. See Procedure 3502, Information Security.

5.6.10 Security of Network Services

Security features, service levels, and management requirements for each network zone must be identified and included in any service level agreement, whether these services are provided in-house or outsourced.

5.7 Handling of Media and Hardcopy

5.7.1 Media and Hardcopy Handling Procedures

Procedures must be drawn up and followed for handling, processing, storing, transporting, transmitting, and disposal or reuse of media and hardcopy. These procedures must be consistent with security guidelines. For details, see Guideline 3502, Information Security.

5.7.2 Encryption of Information on Removable Media

Personal or Confidential information must be encrypted when stored on removable media in accordance with section 2.3 Information Handling and Procedure 3502, Information Security.

5.7.3 Disposal or Reuse of Media

All media must be disposed of or prepared for reuse in such a manner that it is impossible to recover the information. For details, see Procedure 3502, Information Security.

5.7.4 Shredding of Unwanted Hardcopy

Duties and Responsibilities

All hardcopies containing Personal or Confidential information are to be securely shredded when no longer required. See Procedure 3502, Information Security. Where the information constitutes a record, see also Procedure 6701-PR1, Records Management.

5.7.5 *Using External Disposal Firms*

Any external party used for disposal of BCIT's media and hardcopy must have a contractual agreement according to section 1.2.2 Addressing Security in External Party Agreements.

5.7.6 *Security of System Documentation*

System documentation must be protected against unauthorized access.

5.8 Exchange of Information

5.8.1 *Information Exchange Policies and Procedures*

Formal information exchange policies, procedures, and controls must be in place to protect the exchange of information through the use of all types of communication.

5.8.2 *Transmitting Information across Networks*

All Personal or Confidential information must be encrypted in transit, including by email, electronic data interchange, or other forms of interconnection of business systems. Controls must be put in place to verify the integrity of transmitted Personal or Confidential information and the identities of sender and receiver. See Guideline 3502, Information Security.

5.8.3 *Using Fax Machines or Modems*

Personal or Confidential information may only be faxed or sent via public telephone lines where more secure methods of transmission are not feasible. Both the sender and the intended recipient must authorize the transmission beforehand, inform the recipient that the machine should be attended, and confirm the receipt.

5.8.4 *Persons Giving Information over the Telephone*

The identity and authorization of callers must be verified before Personal or Confidential information is provided over the telephone. See Procedure 3502, Information Security.

5.8.5 *Exchange Agreements*

Agreements must be established for the exchange of Personal or Confidential information between the Institute and external parties other than for regulatory or legislative requirements.

5.8.6 *Removable Media in Transit*

Removable media containing information must be protected against unauthorized access, misuse or corruption during transportation.

The transportation of removable media containing Personal or Confidential information must be logged. The removable media must be addressed to the intended recipient and receipt must be confirmed and logged.

Duties and Responsibilities

5.9 Electronic Commerce Services

Controls are necessary to cover the additional security requirements associated with using or providing electronic commerce services.

Information involved in electronic commerce must be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. Electronic commerce systems must meet Payment Card Industry (PCI) standards where appropriate.

5.9.1 *Approval of Electronic Commerce Systems*

Each electronic commerce system requires approval from the Chief Financial Officer (CFO) prior to implementation.

5.9.2 *Personal Payment Information*

All systems storing or processing personal payment information, including credit card numbers and bank account numbers, require approval from the CFO prior to implementation.

5.10 Monitoring

5.10.1 *Logging*

Logs recording security relevant user activities, exceptions, and information security events must be produced and kept for the period specified in the guidelines for access control monitoring and to assist in future investigations. See Guideline 3502, Information Security.

5.10.2 *Monitoring System Use*

Logs, including system and application logs, must be monitored and anomalies investigated. Logs must be reviewed regularly for security events by IT administrators and discrepancies reported to the Information Security Officer. See Procedure 3502, Information Security for details.

5.10.3 *Protection of Log Information*

Logging facilities and log information must be protected against tampering and unauthorized access.

5.10.4 *Administrator and Operator Logs*

IT administrator and other privileged account activities must be logged.

5.10.5 *Clock Synchronization*

System clocks must be synchronized regularly to a common source to simplify the review and correlation of audit logs. The common source is as specified by IT Services. See Procedure 3502, Information Security.

Duties and Responsibilities

6. Access Control

Accounts may be provisioned to provide access to assets including: networks, operating systems, applications, and database management systems. This section governs access to all of these asset categories.

6.1 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.

6.2 User Access Management

Formal user registration and de-registration procedures must be used to grant and revoke access to all information systems and services including network services, operating systems, applications, and database management systems.

The allocation and use of privileges must be restricted and controlled, and the allocation of passwords and other security credentials must be controlled through a formal management process.

6.2.1 *Review of Accounts and Access Rights*

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

6.2.2 *Inactive Accounts*

Inactive accounts must be disabled after the period of inactivity specified in Guideline 3502, Information Security.

6.2.3 *Session Time-out*

Inactive sessions must be terminated after the period of inactivity defined in Guideline 3502, Information Security.

6.2.4 *Additional Access Protections*

Systems may require additional access protections based on time of day, location, and additional authentication requirements. See Guideline 3502, Information Security.

6.3 User Responsibilities

All users must authenticate using their own account for a given system. Approved login procedures must be followed.

6.3.1 *Delegation of Duties*

Where delegation of duties is required to meet a business need, users must employ features within the system wherever possible (e.g., Lotus Notes delegation). Where the system does not provide the ability to delegate, then the procedure for delegating an account through controlled sharing detailed in Procedure 3502, Information Security must be followed.

6.3.2 *Short Term Accounts*

In departments that employ temporary employees on a frequent basis, the use of short term accounts must follow Procedure 3502, Information

Duties and Responsibilities

Security.

6.3.3 *Inadvertent Access to Resources and Information*

Users must not exploit insecure accounts or resources, or take advantage of less knowledgeable users. Users must not read Personal or Confidential information simply because it is accessible to them through accidental exposure or through the malice of others who have broken into a system or are misusing their access privileges. If users discover such an exposure they must report the exposure as a security incident.

6.3.4 *Password Use*

The selection of passwords and their use, protection, and management must follow the corresponding procedures in Procedure 3502, Information Security.

Passwords must not be shared with any other person at any time. The only exception is when authorized users must delegate an account according to Procedure 3502, Information Security.

BCIT passwords must not be used for any non-BCIT accounts or services (such as personal ISP accounts, free online email accounts, instant messaging accounts, or other online services). This practice ensures compartmentalization and reduces the likelihood that passwords obtained from other systems may be used to compromise BCIT systems.

6.3.5 *Controlling Access to Unattended User Equipment*

When leaving a computer or mobile device unattended, users are responsible for:

- Preventing unauthorized access to information and records by either logging off or using device locking software
- Using password protected screen savers to lock workstations and protect the contents of the screen when unattended
- Preventing theft of the computer or device by using a locking device.

All unattended equipment in public areas must be physically secured and configured in a manner such that the security of its systems cannot be easily thwarted.

6.3.6 *Controlling Access to Information in Unattended Areas*

Desks must be cleared of Personal or Confidential information when desks are unattended. Areas that may contain Personal or Confidential information must not be left unattended without securing the information.

Duties and Responsibilities

7. Information Systems Acquisition, Development & Maintenance

7.1 Security Requirements of Information Systems

Statements of business requirements for new information systems, or enhancements to existing information systems must specify the requirements for security controls. Security requirements and controls must reflect the business value of information assets affected by the system and the potential business damage that might result from a failure or absence of security.

System requirements for information security and processes for implementing security should be integrated in the early stages of information system projects. For requirements that must be considered, see Guideline 3502, Information Security.

7.2 Correct Processing in Applications

System owners must ensure that the systems they are responsible for handle information with due care. This includes 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.

7.3 Security in Development, Deployment and Support Processes

Only authorized users may access operational software libraries or the source code of systems. Segregation of duties, technical access controls, and robust procedures must be employed whenever amendments to software are necessary.

7.3.1 *Technical Review of Applications after Execution Environment Changes*

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

7.3.2 *Outsourced Software Development*

Outsourced software development must be in accordance with section 1.2.2 Addressing Security in External Party Agreements.

7.3.3 *Control of Operational Software*

Only authorized users may deploy software on operational systems.

7.3.4 *Using Live Information for Testing*

The use of live information for testing new vendor-supplied or custom systems or system changes may only be permitted where the same controls for the security of the information as used on the production system are in place.

7.4 Technical Vulnerability Management

The ISO and each IT administrator are responsible for monitoring information about the technical vulnerabilities of the information systems, promptly evaluating the Institute's exposure to such vulnerabilities, and taking timely, appropriate measures to address the associated risks. See Guideline 3502, Information Security.

Duties and Responsibilities

8. Information Security Incident Management

8.1 Reporting Information Security Events and Weaknesses

8.1.1 Reporting Information Security Events

All suspected information security incidents must be reported promptly to the Information Security Officer. See Procedure 3502, Information Security for instructions on how to report an information security Incident.

8.1.2 Reporting Security Weaknesses

All information security weaknesses must be reported promptly to the Information Security Officer.

8.2 Management of Information Security Incidents and Improvements

8.2.1 Conduct of Investigations

Information security investigations are coordinated by the Information Security Officer. The ISO is authorized to investigate information security incidents including: seizing Institute-owned equipment, monitoring, and taking images and backups.

8.2.2 Responsibilities and Procedures

BCIT employees and students must provide timely assistance when requested.

External parties' responsibilities for information security incident management must be established according to section 1.2.2 Addressing Security in External Party Agreements.

8.2.3 Investigation Limitations

Investigation of an individual's activities or files by the ISO will only be done in response to an incident or with reasonable suspicion that the individual is engaging in activities that are noncompliant with BCIT policies.

8.2.4 Ensuring the Integrity of Information Security Incident Investigations

To ensure the integrity of evidence, the ISO must be contacted before any investigational activities are undertaken.

8.2.5 Learning from Information Security Incidents

Post-incident review of major incidents must be conducted. Periodically, incidents must be reviewed collectively to identify trends for improvement of security efforts.

Duties and Responsibilities

9. Business Continuity Management

See Policy 7530, Emergency Response for BCIT's business continuity management approach.

9.1 Information Security Aspects of Business Continuity Management

9.1.1 *Including Information Security in the Business Continuity Management Process*

The planning and implementation of business continuity must not compromise information security.

9.1.2 *Disaster Recovery Plan*

System owners must ensure that disaster recovery plans for their systems are developed, tested, and implemented. Recovery time must be negotiated jointly by the system owners and IT Services or other service provider.

Where business requirements exceed the ability to recover IT assets, mitigating controls must be put in place. See Policy 7530, BCIT Emergency Response for more details.

10. Compliance

10.1 Compliance with Legal Requirements

10.1.1 *Intellectual Property Rights (IPR)*

See Policy 6601, Intellectual Property.

10.1.2 *Using Licensed Software*

All software must be appropriately licensed and users must comply with the terms and conditions of all End User License Agreements.

10.1.3 *Protection of Organizational Records*

See Policy 6701, Records Management.

10.1.4 *Data Protection and Privacy of Personal Information*

See section 2.2 Information Classification in this policy.

10.2 Information Systems Audit Considerations

The planning and implementation of information systems audits must not compromise information security.

Access to system auditing tools must be protected to prevent any misuse or compromise.

Duties and Responsibilities

11. Non-Conforming Systems

This policy represents a target environment. Not all systems or technologies are capable of conforming in all details. The Information Security Officer must maintain a list of non-conforming systems and technologies. This is a risk-based activity focusing on non-conforming systems with the highest risk profile.

System owners of systems that are unable to conform to this policy and its guidelines must:

- Report non-conformance to the ISO immediately
- Undertake a risk assessment
- Develop a risk management plan and submit to the ISO.

This exception list will include all systems and technologies that do not conform to this policy and include a reference to the risk assessment and risk management plan for each system or technology on the list. For the complete procedure, see Procedure 3502, Information Security.

12. Consequences of Policy Violation

BCIT 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 the law:

- A verbal or written warning
- Restrictions on or removal of access to any or all Institute computing facilities and services
- Legal action that could result in criminal or civil proceedings
- In the case of students, disciplinary action under Policy 5102, Standards of Non-academic Conduct.
- In the case of 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.

Procedures and Guidelines Associated With This Policy

Procedure 3502, Information Security (to be written)
Guideline 3502, Information Security (to be written)

Forms Associated With This Policy

See Procedure 3502, Information Security (to be written)

Special Situations

None.

Amendment History

1. Created 2009 Jan 27

Scheduled Review Date

2014 Jan 01