Cyber Security

Policy No:	3502
Version:	4
Category:	Information Management
Approving Body:	Board of Governors
Executive Sponsor:	VP Finance & Administration
Department Responsible:	Cyber Security Office
Directory of Records:	0650-15
Approval Date:	2025 Dec 03

Policy Statement

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

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

Who This Policy Applies To

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

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

Consequences of Policy Violation

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

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

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

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

Purpose

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

Roles and Responsibilities

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

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

BCIT Commitment to Cyber Security Risk Management

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

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

security is embedded in all processes and technologies.

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

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

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

Cyber Security Framework Domains

1. Cyber Security Governance

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

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

2. Risk Management

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

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

3. Identity & Access Management (IAM)

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

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

4. IT Asset Management

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

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

4.1 System Categorization

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

5. Data Protection and Privacy

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

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

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

5.1 Information and Data Classification

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

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

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

5.2 Data Retention and Disposal

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

5.3 Secure Transmission and Sharing of BCIT Electronic Data

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

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

5.4 Payment Card Data Security

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

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

6. Encryption

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

For more detailed guidance refer to the ***Encryption Requirement and Cryptographic Controls Standards***.

7. Network Security

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

7.1 IP Address Assignment and Management

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

7.2 Domain Name Management

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

8. Endpoint Security

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

9. Third-Party and Supply Chain Risk Management

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

safeguard Institute assets from unauthorized access, improper use, and operational disruptions.

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

10. User Awareness and Training

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

11. Physical and Environmental Security

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

12. Application Security

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

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

13. Database Security

BCIT must enforce strong security controls across all Institute databases, relational and non-relational, to prevent unauthorized access, data tampering, and unplanned disruptions; ensuring data remains secure, accurate, and reliably accessible. All databases must adhere to recognized cybersecurity frameworks such as National Institute of Standards and

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

14. Vulnerability and Patch Management

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

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

15. Change Management

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

16. Business Continuity Management

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

17. Backup & Disaster Recovery

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

17.1 Redundancy & Infrastructure Resilience

BCIT must design, implement, and maintain redundant and resilient infrastructure to minimize service disruptions from hardware failure, cyber-attacks, or natural disasters. Infrastructure supporting mission-critical services must also include failover capabilities, and geographic distribution to ensure continuity and integrity. For more detailed guidance refer to the ***Backup and Recovery Management Standard*.**

18. Incident Response & Monitoring

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

18.1 Incident Response & Activation

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

18.2 Emergency Authority

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

19. Cloud Security

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

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

operational risks. For more detailed guidance, reference the ***Cloud Security and Compliance Standard*.**

20. Human Resources Security

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

21. Email Security & Privacy

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

22. Compliance and Monitoring

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

23. Exceptions

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

subject to periodic review, at least biannually or upon any significant system or operational changes.

APPENDICES

A. Technical Standards Associated with This Policy

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

B. Amendment History

	Approval Date	Status
1. Created: Policy 3502 version 1	2009 Jan 27	Replaced
2. Revised: Policy 3502 version 2	2016 Oct 04	Replaced
3. Revised: Policy 3502 version 3	2020 May 26	Replaced
4. Revised: Policy 3502 version 4	2025 Dec 03	In Force

C. Scheduled Review and Updates

This policy must be reviewed no later than five years from approval (2030 December 3). However, it may be updated as needed to address emerging threats and changes in technology or regulatory requirements.

D. Definitions

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

Term	Definition
Confidential Information	Any data or information that is meant to be kept private and secure, and whose unauthorized access, disclosure, or exposure could harm individuals or BCIT.
Contact Information	Means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone numbers, business address, business email or business fax number of the individual.
Contractors	An individual or entity engaged under contract to perform specific work or services for BCIT, and who may require access to BCIT systems, facilities, or information assets during the course of their engagement.
CSO	Cyber Security Office.
Data	Data refers to raw, unprocessed facts, figures, or symbols that are collected, generated, or received by BCIT systems, individuals, or processes. Data may exist in digital, physical, or verbal form and becomes information when it is organized, interpreted, or contextualized to convey meaning.
Disaster Recovery	The activities that restore the Institute to an acceptable condition after suffering a disaster. See Policy 7110, Emergency Management for more information.
Encryption	The conversion of information or data into a coded format to make it unreadable to prevent unauthorized access.
End Users	Individuals who interact with the system, application, or service on a daily basis. They are the final point of interaction in the technology chain and are usually not involved in the development or maintenance of the system.
ERM	BCIT Enterprise Risk Management
FIPPA	*Freedom of Information and Protection of Privacy Act* (BC)
Firewall	A system designed to prevent unauthorized access to or from a private network or between network zones.
GDPR	General Data Protection Regulation.
Information	Refers to all forms of institutional knowledge, data, and record, whether digital, physical, or verbal, that are created, stored, transmitted, or processed by BCIT. Information is considered an asset and must be protected against unauthorized access, disclosure, alteration, or destruction to preserve its confidentiality, integrity, and availability.
Information Security	The preservation of confidentiality, integrity, and availability of information. Confidentiality ensures that information is accessible only to authorized users. Integrity involves safeguarding the accuracy and completeness of information and processing methods. It may also include authenticity, auditability, accountability, non-repudiation, and reliability of information. Availability ensures that Authorized Users have access to IT assets when required.
Information Security Classifications	The information security categories are described in section 5.1 *Information Security Classifications.*

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

E. Related Documents and Legislation

Law/Regulation/Policy	Document Name
BC legislation	*College and Institute Act*, RSBC 1996, c 52 *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 *Personal Information Protection Act*, SBC 2003, c 63
Federal legislation	*Criminal Code*, RSC 1985, c C-46 *Copyright Act*, RSC 1985, c C-42 Canada's Anti-Spam Legislation (i.e. CASL)[1]

Law/Regulation/Policy	Document Name
Industry Standards	PCIDSS, Payment Card Industry Security Standards published by the Payment Card Industry Security Standards Council, including the "PCI Data Security Standard", the "PIN Transaction Security Requirements", and the "Payment Application Data Security Standard" NIST 800-82 (Guide to Industrial Control Systems Security) IEC 62443 (Industrial Automation and Control System Security) NERC CIP (Critical Infrastructure Protection for energy systems) ISO 27001 (Information Security Management Systems) CIS Controls (Control 07: Continuous Vulnerability Management) NIST SP 800-40 Rev. 3, NIST SP 800-53, NIST SP 800-37 Rev. 2 CIS Controls v8 (Control 16: Application Software Security) NIST SP 800-218 (Secure Software Development Framework - SSDF) OWASP Top 10
BCIT Policies	1500, Code of Conduct 3501, Acceptable Use of Information Technology 5102, Student Code of Conduct (Non-Academic) 5900, Education Technology 6601, Intellectual Property 6700, Freedom of Information and Protection of Privacy 6701, Records Management 7506, Use of Materials Protected by Copyright 7170, Protection of Equipment and Property 7110, Emergency Management