Policy Information	
Policy No:	AD-IT-6.03
Approved by:	Executive Committee
Approval Date:	November 18, 2020
Executive Responsible:	VP Finance and Corporate Services
Administrator Responsible:	Chief Information Officer
Date of Next Review:	November 2021

INFORMATION CYBERSECURITY

Policy Statement

The College of New Caledonia (CNC) will proactively assess and mitigate cyber risks by implementing an information and cybersecurity framework consisting of policies, procedures, technology, and other resources to ensure the safety of the College's information.

Purpose / Rationale

This policy has been developed to:

- Protect the confidentiality, integrity, and availability of CNC information and associated information technology.
- Provide management with direction and support for information cybersecurity in accordance with business requirements and relevant laws and regulations.
- Define the roles of individuals and organizational entities involved in information cybersecurity and establish the responsibilities of these roles.
- Ensure the reliable operation of CNC's information technology so that all members of the CNC community have access to the information assets they require.

Scope / Limits

This policy applies to all CNC information, computing, communications, and networking resources and the users of these resources. CNC's information, network, and other IT services are shared resources that are critical to teaching, learning, research, college operations, and service delivery.

Principles/Guidelines

1. By nature, a post-secondary educational institute needs to share information for the purpose of delivering education. Cybersecurity measures must be implemented in a manner that enables appropriate information exchange.

2. Cybersecurity is a shared responsibility and accountability across the College.

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 that information.

4. Users will be provided sufficient training to allow them to properly protect information assets.

5. Cybersecurity controls must be cost-effective and in proportion to the risks and the value of the assets that need to be protected.

6. Cybersecurity is multi-disciplinary and requires a comprehensive and integrated approach covering every aspect of CNC's operations.

7. All parties should act in a timely, coordinated manner to prevent and respond to cybersecurity incidents.

8. Cybersecurity must be periodically assessed to ensure that adequate measures are in place to protect the assets of CNC.

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 will be employed to reduce the risk of failure of any single measure (defense 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 privacy protection in mind. Where adequate cybersecurity cannot be achieved through technical means, alternate controls must be implemented.

Duties and Responsibilities

1. Each user within the CNC community will make reasonable cybersecurity arrangements to protect information resources for which the member is responsible including:

   a. Taking appropriate measures to prevent loss, damage, abuse, or unauthorized access to information assets under their control.

b. Promptly reporting all acts that may constitute real or suspected breaches of cybersecurity including, but not limited to, unauthorized access, theft, system or network intrusions, willful damage, and fraud.

c. Responsible for 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 engaging in College activities.

d. Respecting the classification and curation of information.

e. Complying with all the cybersecurity requirements defined in this policy.

f. Complying with other related policies including Acceptable Use of CNC Information Technology Policy AD-IT-6.02.

g. Ensuring the data and systems they work with are secure.

2. The College holds and processes information about employees, students, and other data subjects for academic, administrative and commercial purposes. When handling such information, the College, and all those to whom this Policy applies, must comply with the BC Freedom of Information and Protection of Privacy Act (FOIPPA) and any privacy policy specific to the College.

3. The Chief Information Officer will establish an Information Cybersecurity Framework including specific policies, standards or procedures to ensure privacy protection with regard to college related information.

4. To maintain the privacy of the College's Information, users intending to conduct college business using systems other than sanctioned college systems must receive explicit permission from the Chief Information Officer to do so.

5. The Chief Information Officer will investigate suspected violations of this policy and recommend or implement corrective action, suspend, disable, terminate, or remove access to or from information resources, or take other action in accordance with collective agreements and college policies and procedures.

6. Access to CNC information assets, except public assets, must not be granted to external parties without an information sharing agreement or other contractual agreement.

Definitions

1. Asset
   Anything that has value to the College.

2. Compartmentalization
   The limiting of access to information to persons or other entities on a need-to-know basis to perform certain tasks.

3. 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. College data is all data related to, received by, or created by CNC.

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

5. Incident
   An identified occurrence of a system, service, or network state indicating a possible or pending breach of information cybersecurity or breach of acceptable use or failure of safeguards or a previously unknown situation that may be cybersecurity relevant.

6. Information
   Includes all forms of data, documents, records, communications, conversations, messages, recordings, and photographs. It includes everything from digital data to paper records and telephone conversations.

7. Information Asset
   An asset that is comprised of information or of equipment or systems for the processing of information.

8. Information Privacy
   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. Availability ensures that authorized users have access to information assets when required.

9. Information Cybersecurity Framework
   A comprehensive approach to preserve information privacy including: Risk assessment and impact analysis, guiding principles, policies, guidelines, and procedures, controls and countermeasures, information cybersecurity awareness including education and training

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

11. Personal Information
    As defined in Freedom of Information Protection of Privacy Act.

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

13. User
    A person who performs any action on an information asset.

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

Legislative and Collective Agreement References

BC Colleges and Institutes Act
BC Freedom of Information and Protection of Privacy Act (FOIPPA)
CNC Faculty Association Collective and Common Agreements
CNC CUPE Collective Agreement

Links to Other Related Policies, Documents and Websites

Acceptable Use of CNC Information Technology Policy AD-IT-6.02

Policy Amendment Log

Amendment Number:	Date:
0	November 2020
1	
2	