

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.

- x Provide management with diremembers of the CNC community have access to the information assets require.

Scope / Limits

This policy applies to all CNC information, computing, communications, and networking resources and the users of these resources.

- 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

9. Information Cybersecurity Framework

A comprehensive approach to preserve information privacy including: Risk procedures, controls and awareness including education

10. Least Privilege

The principle that requires

11. Personal Information

As defined in Freedom of

12.