COQUITLAM COLLEGE
Established 1982

POLICY AND PROCEDURES

POLICY NAME:	POLICY NUMBER:	CATEGORY:
Information Security	1.2.3	Administration
RESPONSIBLE EXECUTIVE:	APPROVAL AUTHORITY:	EFFECTIVE DATE:
Privacy Officer	Senior Leadership Team	October 11, 2023
NEXT FULL REVIEW DATE:	REVISED:	REPLACES:
October 10, 2028		

Purpose
The purpose of this policy is to establish consistent practices and guidelines regarding the confidentiality, integrity and availability of information, and the management of access to information by employees of Coquitlam College (the College).

Scope
This policy applies to all employees of the College.

Policy Statements
1. The College will apply appropriate measures to support and maintain information security and IT systems and will implement a rigorous process regarding access to and the security of data.

2. The College provides a safe and secure environment for the collection, storage, access and retrieval of information.

3. College Data is all information that is collected, maintained and utilized by the College for the purpose of carrying out operations. College data falls into three classifications:

   a. Class 1 – Public: Data that is or can be publicly released without causing any harm to the College or a person.

   b. Class 2 – Internal: Data that if released may cause minor harm or embarrassment to the College or a person.

   c. Class 3 – Confidential: Data that if compromised can cause considerable harm or embarrassment to the College or a person.

4. The College will apply the Least Privilege Protocol and Need to Know Principle when assessing and allowing access to information.

5. Employees are expected to handle information related to College business and activities responsibly within their respective roles and in accordance with policies, procedures, and associated regulations.

6. Employees must not access any information they do not need to perform their business responsibilities, regardless of whether this information is accessible to them.

7. Employees found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

Procedures

8. Before the commencement of projects that will utilize college data, the below roles must be assigned to individuals within the project by the relevant supervisor of that project or their reasonable designate as assigned by the President.

Roles and responsibilities

9. College Administrators
   Senior officials of the College responsible for:
   - Establishing and maintaining an appropriate information management system
   - Providing ongoing executive oversight of information management systems
   - Ensuring that employees are aware of and follow their information security responsibilities

10. Data Trustee
    Institutional officers responsible for:
    - establishing and maintaining guidelines, policies and procedures regarding data access and usage within their authority
    - determining the appropriate classification of data and information and providing this information to Data Users
    - where appropriate, establishing rules for data users to classify information

11. Data Custodian
    An individual responsible for granting appropriate access to users.

12. System Owner(s) are responsible for:
    - Assessing security requirements for systems
    - Ensuring that data processes on systems remains secure, including configuring the security features of a system in accordance with relevant policies, standards, guidelines and legislation
    - Properly storing, protecting, enabling use, and backing up of data and systems
    - Ensuring systems are designed, configured, implemented, operated, maintained, upgraded, and decommissioned consistent with established security standards

13. Data User
    Employees granted access to institutional data and/or systems in order to perform assigned duties and fulfill assigned roles or functions within the College. Data users are responsible for:
    - Taking appropriate measures to prevent loss, damage, abuses, or unauthorized access to information under their control
    - Secure storage and disposal of confidential documents in paper and portable media format in their custody

- Respecting the classification of information as established by a Data Trustee and/or classifying information created by them per the rules established by a Data Trustee
- Complying with all data security requirements set out by College guidelines, policies, procedures and practices

Definitions

Employee: An individual who is employed by the College on a full-time, part-time, permanent, temporary or contract basis.

Least Privilege Protocol: Individuals are granted only those privileges they need to perform their work tasks and job functions.

Need to Know Principle: Individuals are provided with only that information they need to perform their work tasks and job functions and at the time they need to know it.

Related Documents
- 1.2.1 Personal Information and Protection of Privacy Policy for Students
- 1.3.9 Personal Information and Protection of Privacy for Employees and Volunteers
- Personal Information Protection Act (PIPA)