


Procedure Name:	COLLEGE DATA CLASSIFICATION	
Approved By:	Board of Governors	
Approval Date:	September 5, 2025	
Next Scheduled Renewal Date:	August 2030	
Procedure Holder:	VP, Corporate Services & CFO	
Operational Lead:	Director, Information Technology/CIO	
Procedure Number:	INF-005P	

COLLEGE DATA CLASSIFICATION PROCEDURE

1.00 PURPOSE

- 1.1 The purpose of this procedure is to set the minimum standards necessary for classifying various types of College data so that reasonable security arrangements can be applied to such information.

2.00 DEFINITIONS

- 2.1 **Data:** Information in any form, digital or physical, that the College creates, receives, or manages. It may include student records, research results, financial details, or operational information. Data must be protected according to its sensitivity, value, and legal requirements.
- 2.2 **Data Auditor:** The individual responsible for reviewing a Data Owner's classification to determine if it aligns with regulatory or other corporate requirements and business objectives. The Data Auditor is also responsible for reviewing the data users' effective handling of data in accordance with the appropriate policies, procedures and legislation. This is often a privacy officer or the Director of IT & Chief Information Officer (CIO).
- 2.3 **Data Creator:** An individual who creates new data and is responsible for classifying it as it is created. The Creator should assess the severity of the organizational impact if that data was compromised to efficiently decide on the classification. Anyone within the organization can be a data creator.
- 2.4 **Data Custodian:** An individual responsible for the safe custody, transport, and storage of the data and implementation of business rules and policies. For electronic records this role is often performed by the Information Technology (IT) Department.
- 2.5 **Data Owner:** An individual, often a department manager (or a similar role), who has direct responsibility for the data that resides and/or is primarily used within their department. The owner is accountable for classifying the data and reviewing the classification.
- 2.6 **Data Steward:** The individual responsible for data governance, practices, and requirements – essentially responsible for the entire data classification program.
- 2.7 **Data User:** An individual who accesses data at any point during its lifecycle. Anyone within the organization can be a data user.

- 2.8 **Individuals:** Often department heads (or a similar role), who have direct responsibility for the data and controlling access to data for designated systems.
 - 2.9 **Information Resources:** Any devices, assets, and infrastructure owned by, explicitly controlled by, or in the custody of the College, including but not limited to data, records, electronic services, network services, software, computers, laptops, tablets, smartphones, mobile computing devices, and information systems.
 - 2.10 **The College:** Coast Mountain College.
- 3.00 ASSIGNING AN INFORMATION SECURITY CLASSIFICATION LEVEL
- 3.1 Information resources require security classification at the level appropriate for them, in accordance with the classification levels set out in Section 5.00.
 - 3.2 The security classification level of the information resource establishes the extent and type of security arrangements that must be implemented to protect the information resource.
 - 3.3 Security classification levels are applied to broad information types or categories, rather than individual records.
 - 3.4 Before assigning a security classification level, departments must be aware of any relevant legislative requirements, regulatory obligations, and College policies and procedures.
 - a. Departments may also refer to various guidelines, standards, and best practices for further direction, where applicable.
 - 3.5 Where it is unclear which security classification level is most appropriate or when dealing with large volumes of information, the highest appropriate classification level should be used.
 - 3.6 Where an information system or record contains information that is classified as public as well as information classified at a higher level, the combined information must be managed at the higher confidentiality level.
 - 3.7 In deciding which security classification level is most appropriate, Departments must consider the volume of information and should consider using a higher classification level.
 - a. An increase in risk due to volume may necessitate using a higher security classification level.
- 4.00 RESPONSIBILITIES
- 4.1 Departments are expected to classify and manage information resources for which they are responsible based on a reasonable understanding of the overall value of the resource.
 - a. Where appropriate, the Department may need to collaborate with other teams to classify and manage the information resources for which they are responsible.
 - 4.2 Department Leaders are expected to ensure that Users in their units manage information resources according to the assigned security classification.

- 4.3 For data received from external institutions or partners, the College department receiving the data assumes accountability as the Data Owner within the College environment.

5.00 CLASSIFICATION LEVELS

- 5.1 Data resources are classified according to the levels in Table 1.
 - a. **Level 4 Classification (Highly Confidential):** Data that is intended for use only by authorized personnel, and unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the College and/or national security.
 - b. **Level 3 Classification (Confidential):** Data that must be kept private under federal, local, and state laws, contractual agreements, or based on its proprietary worth.
 - c. **Level 2 Classification (Internal):** Data that is not openly published but can be made available via open record requests. Direct access to this data is restricted to authenticated and authorized employees. Limited data may contain redactions to protect confidential material.
 - d. **Level 1 Classification (Public):** Data that is readily available to the public with anonymous access.
- 5.2 Prohibited Information:
 - a. In addition to the classification levels identified in Table 1, certain information may be deemed by industry regulations, legislation, or other mechanism to be prohibited.
 - b. Such information may not be collected or stored by the College in any form.

Table 1: Coast Mountain College Data Classification Levels.

	Level 4	Level 3	Level 2	Level 1
Definition	Information resource is so sensitive or critical that it is entitled to extraordinary protections, as defined in Section Error! Reference source not found.	Information resource is considered to be highly sensitive business or personal information, or a critical system. It is intended for a very specific use and may not be disclosed except to those with explicit authorization to review such information, even within a workgroup or unit.	Information that is intended for use within the College or within a specific department, unit or group of individuals with a legitimate need-to-know. Internal information is not approved for general circulation outside the workgroup or unit.	Information that has been approved for distribution to the public by the data owner or through some other valid authority such as legislation or policy.
Legal Requirements	Protection of information where it is required by law or regulation (e.g., FOIPPA), or as determined by contractual obligation.	The College has a contractual or legal obligation to protect the information.	The College has a contractual obligation to protect the information.	Information may be mandated by legislation to be public information.
Reputational Risk	Critical loss of trust or credibility. Significant media attention. College staff require special training and processes to deal with the data.	Significant loss of trust or credibility. Guaranteed to generate media attention and increased scrutiny.	Potential for lost trust or credibility. May generate some media attention and result in increased scrutiny.	No impact on reputation.
Operational Risk	Risk will render the College unable to achieve its overall objective or mandate.	Significant impact on the College's ability to achieve its objectives.	Moderate impact on the College's ability to achieve its objectives.	Little or no impact on the College's ability to achieve its objectives.
Financial Risk	Major revenue loss or impact on College budget or may result in fines.	Significant revenue loss or impact on College budget or may result in fines.	Minor negative financial impact for the College or department.	Impact is within normal operating budget margin fluctuations.
Disclosure Risk	Highly adverse negative impact on the College or individuals, including identity theft.	Moderately adverse negative impact on the College or individuals.	Possible adverse impact on the College or Individuals.	Disclosure of public information requires no further authorization and may be freely disseminated without potential harm to the College.

6.00 SECURITY ARRANGEMENTS FOR CLASSIFICATION

6.1 After an information security classification level has been applied, reasonable security arrangements are required that correspond to the assigned level. Table 2 sets out appropriate safeguards for each level of information.

Table 2: Security Arrangements by Classification Level.

	Level 4	Level 3	Level 2	Level 1
Access	<ol style="list-style-type: none"> 1. Access is limited to specific named individuals or positions. 2. Principles of least privilege and need-to-know must be applied. 3. Access must be revoked immediately when users leave the College or transfer to another College department. 	<ol style="list-style-type: none"> 1. Access is limited to individuals in a specific function, group, or role. 2. Principles of least privilege and need-to-know must be applied. 3. Access must be revoked as soon as reasonably possible when users leave the College or transfer to another College department. 	<ol style="list-style-type: none"> 1. Access is limited to employees and other authorized users for business-related purposes. 2. Access must be revoked as soon as reasonably possible when users leave the College or transfer to another department. 	<ol style="list-style-type: none"> 1. No access restrictions.
Transmission	<ol style="list-style-type: none"> 1. Encryption for public networks (e.g., wireless, Internet). 2. Encryption is strongly recommended on trusted, internal networks. 3. Third-party email providers are not appropriate for transmitting. 4. Data may be masked instead of encrypted. 5. Double envelope mailings for hardcopy records. 	<ol style="list-style-type: none"> 1. Encryption for public networks (e.g., wireless, Internet). 2. Encryption is strongly recommended on trusted, internal networks. 3. Third-party email providers are not appropriate for transmitting. 4. Data may be masked instead of encrypted. 5. Clearly marked "Confidential" on sealed mailings. 	<ol style="list-style-type: none"> 1. Encryption is strongly recommended on public networks (e.g., wireless, Internet). 	<ol style="list-style-type: none"> 1. No special handling required.
Storage	<ol style="list-style-type: none"> 1. Stored within a controlled-access system (e.g., password protected file or file system, locked file cabinet, alarmed area). Additional controls implemented as necessary to comply with relevant legislation or other requirements. 2. Encryption mandatory on mobile devices and workstations, and strongly recommended in all environments. 3. Implement clean desk policy. 4. Must be stored in Canada. 	<ol style="list-style-type: none"> 1. Stored within a controlled-access system (e.g., password protected file or file system, locked file cabinet, alarmed area). 2. Encryption mandatory on mobile devices and workstations, and strongly recommended in all environments. 3. Implement clean desk policy. 4. Must be stored in Canada. 	<ol style="list-style-type: none"> 1. Stored within a controlled access system (e.g., password protected file or file system, locked file cabinet). 2. Encryption strongly recommended in all environments. 	<ol style="list-style-type: none"> 1. No special handling required.
Destruction	<ol style="list-style-type: none"> 1. Shredded or erased in accordance with the College's policy for the secure destruction of information. 	<ol style="list-style-type: none"> 1. Shredded or erased in accordance with the College's policy for the secure destruction of information. 	<ol style="list-style-type: none"> 1. Shredded or erased in accordance with the College's policy for the secure destruction of information. 	<ol style="list-style-type: none"> 1. No special handling required.

7.00 RELATED POLICIES, PROCEDURES, AND GUIDELINES

- 7.1 ADM-005G, *Guideline for the Secure Destruction and Deletion of College Records and Information*
- 7.2 [ADM-011, Records Management Policy](#)
- 7.3 [ADM-018, Enterprise Risk Management Policy](#)
- 7.4 INF-005P, *College Data Classification Policy*

8.00 OTHER SUPPORTING DOCUMENTS

- 8.1 [BC Freedom of Information and Protection of Privacy Act](#)
- 8.2 CMTN [Enterprise Risk Management Framework](#)
- 8.3 [CMTN Risk Register](#)
- 8.4 *Data Collection Standard (CMTN)*
- 8.5 [PCI-DSS Quick Reference Guide](#)

9.00 HISTORY

Created/Revised/ Reviewed	Date	Author's Name and Role	Approved By
Created	Sept. 5, 2025	Director, Information Technology/CIO	Board of Governors