


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

COLLEGE DATA CLASSIFICATION POLICY

1.00 PURPOSE

- 1.1 The purpose of this policy is to define how data is identified, classified, labeled, and securely handled and protected in accordance with its importance and potential impact to Coast Mountain College (the College).

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 **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.
- 2.9 **The College:** Coast Mountain College (CMTN).
- 3.00 POLICY STATEMENT
 - 3.1 Data must be properly handled throughout its entire lifecycle, from creation to disposal. The importance of such information varies and therefore requires different levels of protection.
- 4.00 SCOPE
 - 4.1 This policy applies to all College employees, contractors, volunteers, Board of Governors members, and any other users authorized to access data stores, information in any medium, and/or information systems.
 - 4.2 In addition, third parties may be subject to this policy through contractual obligations to the College.
- 5.00 GUIDING PRINCIPLES
 - 5.1 At Coast Mountain College, depending on departmental size and capacity, individuals may hold more than one role (e.g., data owner and data creator, or data steward and data custodian). The responsibilities of each role remain distinct, even if carried out by the same person.
 - a. To preserve independence, the data auditor will not also serve as the data owner for the a single dataset.
 - 5.2 A team of IT Members and Data Owners will oversee the data classification initiative in accordance with this policy and its accompanying procedure (INF-005P, *College Data Classification Procedure*).
 - 5.3 Data Owners (often based on departments) will identify a data steward, who works with the Information Technology (IT) Department to establish and enforce a data classification (DC) standard for adoption by the College.
 - 5.4 Each department will identify and classify its information systems and data stores and manage access to those systems and stores in compliance with the adopted DC standard.
 - 5.5 Data classification will indicate the level of impact to the College if the confidentiality, integrity, and/or availability of the information is compromised.
 - a. If the appropriate classification of an asset is not obvious (i.e., not dictated by specific laws and regulations), use Table 1 as a guide to effectively classify the asset.
 - b. The higher the impact on the College, the more restrictive the classification should be.
 - 5.6 Departments will ensure that all non-public data is appropriately identified, including restrictions on redistributions when transmitted via email or physical mail, which are to be adopted using the DC standard.

- 5.7 The Data Steward, with assistance from Data Custodians as needed, will establish a department-wide data-handling training curriculum.
- 5.8 Data Custodians will:
 - a. review the department's progress annually
 - b. monitor or evaluate the metrics annually
 - c. work with IT to ensure appropriate asset protection measures are in place relative to the data's classification.
- 5.9 The Data Auditor will review data classifications semi-annually to determine if previous data classifications can be safely downgraded to a lower classification level.
- 5.10 College employees, members of the Board of Governors, Contractors, Volunteers, and any other Users authorized to access data stores, information in any medium, and/or information systems will comply with the information asset handling standards established in the DC standard.

6.00 CLASSIFICATION LEVELS

- 6.1 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. See Table 1 for details.
 - b. **Level 3 Classification (Confidential):** Data that must be kept private under federal, local, and provincial laws, contractual agreements, or based on its proprietary worth. See Table 1 for details.
 - 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. See Table 1 for details.
 - d. **Level 1 Classification (Public):** Data that is readily available to the public with anonymous access. See Table 1 for details.

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 6.1 a.	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.

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 Procedure*

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 Services	Board of Governors