Standard for Security Classification of College Information

Parent Policy:	*Use of Information Technology Resources*		
Standard Sponsor:	College Information Officer		
Standard Contact:	Manager, IT Client Services		
Stakeholders:	Okanagan College Users		
Approved by:	College Information Officer		
Effective Date:	29-April-2024		
Last reviewed:	29-April-2024	Scheduled review date:	29-April-2025

1. Purpose

1.1 College’s information used by employees, students, and the public (users) has varying degrees of sensitivity which have corresponding levels of risk and protection requirements. As such, it is necessary to classify this information to ensure it has the appropriate level of protection.

1.2 All College information is covered under this security standard.

1.3 College information is classified using a four-level Information Security Classification Model outlined below. The appropriate security classification assesses the integrity, availability, sensitivity and/or value of data and information. Security classifications are utilized to make decisions to disclose or share information externally as well as inform the storage specifics related to the data's classification.

1.4 The classification of information may change over time due to changing circumstances. Based on other relevant factors, information may be reclassified at a higher level than indicated in the classification table below, but not downgraded to a lower level.

2. Information Security Classification Model

College Information is classified as follows:

Definition	Examples	Potential Impact of Loss
Low Risk		
College information that would cause minimal harm if disclosed, or may be freely disclosed	Names and work contact information of College faculty and staff members Information that is posted on our public website Research information of a non-personal, non-proprietary nature	Minor embarrassments, minor operational disruptions
Medium Risk		
College information that is not protected by law or industry regulation from unauthorized access, use or destruction, but could cause harm to the College or others if released to unauthorized individuals	Proprietary information received from a third party under a non-disclosure agreement. Restricted circulation library materials Confidential financial information and records Information that could allow somebody to harm the security of individuals, systems or facilities. Research information of a non-personal, proprietary nature Proposals for competitive bids	Reputational and financial impact, loss of priority of publication, loss of competitive grant bids, loss of access to copyrighted materials
High Risk		
College information that must be protected by law or industry regulation from unauthorized access, use or destruction, and could cause moderate harm if disclosed	Personal Information, which must be protected under the BC Freedom of Information and Protection of Privacy Act (FIPPA), including: Full face photographic images Student name Student or Employee ID	Moderate harm to one or more individuals, identity theft, impact to College reputation or operations, financial loss such as regulatory fines and increased credit card transaction fees

	Student grades Home address	
Very High Risk		
College information that must be protected by law or industry regulation for unauthorized access, use or destruction, and could cause significant harm if disclosed	Social Insurance Number (SIN) Official government identity card (e.g. Passport ID, Driver's License No.) Bank account information (e.g., direct deposit details) Personal Health Information (PHI) Biometric data Personally identifiable genetic data Date of Birth (DoB) Payment Card Industry (PCI) Information, which must be protected under the Payment Card Industry – Data Security Standard (PCI-DSS) (e.g. credit card numbers, names, expiry dates or PINS)	Significant harm to one or more individuals, identity theft, severe impact to College reputation or operations, financial loss such as regulatory fines or damages from litigation.

3. Access Control, Transmission, Storage, and Disposal

College Information management activities as follows:

Access Restrictions	Transmission	Storage	Disposal
Low Risk			
No restrictions on access	No special handling required Refer to Transmission and Sharing of College Electronic Information	No special safeguards	Can be recycled, erased
Medium Risk			

Access limited to employees and other authorized users	No special handling required Refer to Transmission and Sharing of College Electronic Information	Stored within a controlled access system. Examples: Password protected file or a files system or locked file cabinet	Shredded, securely erased
High Risk / Very High Risk			
Access limited to authorized users with a demonstrated need to know.	Encryption required for external networks. Hard copies must use secure methods for external transportation Refer to Transmission and Sharing of College Electronic Information	Stored within a controlled access system within locations defined by the Director, IT Services and Privacy Officer. Example: Password protected files of file system or locked file cabinet. For any portable medium such as USB drives, notebooks, tablets, and smart phones - encryption required.	Shredded, pulped, degaussed (removal of magnetic information), or securely destroyed

4. Responsibilities

4.1 Leadership Council members are responsible for knowing the types of College information under their control, its information security classification and where it is stored. To comply with our legal obligations, it is recommended that the Leadership Council members maintain an inventory of types of records that contain high risk and/or very high risk information. At a minimum, the inventory should contain the type of information, description and storage location.

4.2 Questions about this standard may be referred to itsecurity@okanagan.bc.ca

History / Revisions

Date	Action
2024-04-29	*New Standard Approved by: College Information Officer*