a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #01
Security Classification of UBC Electronic Information

Introduction

1. UBC Electronic Information used by Users, has varying degrees of sensitivity which have corresponding levels of risk and protection requirements; therefore, it is necessary to classify this information to ensure it has the appropriate level of protection.
2. This standard explains how UBC Electronic Information is classified using UBC's four-level Information Security Classification Model.
3. The Chief Information Officer has issued this document under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.
4. This standard applies to all UBC Electronic Information.

Information Security Classification Model

5. UBC Electronic Information is classified as follows:

Definition	Examples	Potential Impact of Loss
Low Risk		
UBC Electronic Information that would cause minimal harm if disclosed, or may be freely disclosed	• Names and work contact information of UBC faculty and staff members • Information that is posted on our public website • Research information of a non-personal, **non-proprietary** nature	Minor embarrassment, minor operational disruptions
Medium Risk		
UBC Electronic Information that is not protected by law or industry regulation from unauthorized access, use or destruction, but could cause harm to UBC or others if released to unauthorized individuals	• Proprietary information received from a third party under a non-disclosure agreement • Restricted circulation library journals • 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	Reputational and financial impact, loss of priority of publication, loss of access to journals and other copyrighted materials
High Risk		
UBC Electronic 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 *Freedom of Information and Protection of Privacy Act*, including: ▪ Full face photographic images ▪ Student name ▪ Student or Employee ID ▪ Student grades ▪ Home address ○ Payment Card Industry (PCI) Information, which must be protected	Moderate harm to one or more individuals, identity theft, impact to University reputation or operations, financial loss, such as regulatory fines and increased credit card transaction fees

Definition	Examples	Potential Impact of Loss
	under the Payment Card Industry – Data Security Standard (PCI-DSS) (e.g. credit card numbers, names, expiry dates, or PINs)	
Very High Risk		
UBC Electronic Information that must be protected by law or industry regulation from 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)	Significant harm to one or more individuals, identity theft, severe impact to University reputation or operations, financial loss, such as regulatory fines or damages from litigation

6. The classification of information may change over time. For example, unpublished research data may be classified as Medium Risk, but after publication, it may change to Low Risk.

Responsibilities

7. The Information Steward/Owner is responsible for determining the information security classification based on the definitions and examples in the table above. Based on other relevant factors, information may be classified at a higher level than indicated above, but not at a lower level.

8. The Administrative Head of Unit is responsible for knowing the types of UBC Electronic Information under their control, its information security classification and where it is stored. In order to comply with our legal obligations, it is recommended that the Administrative Head of Unit keep 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. Refer to the sample inventory attached to this standard. This responsibility may be delegated to the Information Steward/Owner.

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

What is Personal Information? [Privacy Fact Sheet]

How different combinations of information can affect risk [Privacy Fact Sheet]

Sample Inventory