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 three-level Information Security Classification Model.
3. The Chief Information Officer has issued this document under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

Information Security Classification Model

4. UBC Electronic Information is classified as follows:

	Confidential	Sensitive	Public
Definition	UBC Electronic Information that must be protected by law or industry regulation from unauthorized access, use or destruction	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	UBC Electronic Information that may be freely released to the public

Examples	• Personal Information, which must be protected under the *Freedom of Information and Protection of Privacy Act.* Examples:
	  • Official government identity card No. (e.g. Social Insurance No., Drivers' License No.)
	  • Bank Account Information
	  • Personal Health Information (PHI)
	  • Biometric data
	  • Full face photographic images
	  • Date of Birth (DoB)
	  • Student name
	  • Student or Employee ID
	  • Student grades
	  • Home address
	• 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)
		• Proprietary information received from a third party under a non-disclosure agreement
		• Restricted circulation library journals
		• Research information of a non-personal nature
		• Financial information and records
		• Information that could allow somebody to harm the security of individuals, systems or facilities
		• Any information that is not Confidential and is not generally made available to the public
			• Names and work contact information of UBC faculty and staff members
			• Information that is posted on our public website

Potential Impact of Loss	High (e.g. significant harm to one or more individuals, identity theft, severe impact to University reputation or operations, financial loss, such as fines of up to $500,000, increased credit card transaction fees)	Moderate (e.g. reputational and financial impact, loss of priority of publication, loss of access to journals and other copyrighted materials)	Low (e.g. minor embarrassment, minor operational disruptions)

Responsibility for Classifying Information

5. The Administrative Head of Unit is responsible for creating an inventory of all UBC Electronic Information under his/her control and determining its information security classification. This responsibility may be delegated to the Information Steward/Owner.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems