THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U1
Security Classification of UBC Electronic Information and Services

1. Introduction

1.1 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.

1.2 UBC Electronic Services have varied risk based on their confidentiality, integrity and availability requirements to University operations and the volume and nature of the UBC Electronic Information they process; therefore, it is necessary to classify services to ensure they have appropriate level of protection.

1.3 This standard explains how UBC Electronic Information and UBC Electronic Services are risk classified.

1.4 The Chief Information Officer has issued this standard 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.

1.5 This standard applies to all UBC Electronic Information and UBC Electronic Services.

2. Information Security Risk Classification Model

2.1 UBC Electronic Information is classified as follows:

Definition	Examples	Potential Impact of Loss
Low Risk Information		
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 Information		
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 Information		
UBC Electronic Information that must be protected by law or industry regulation from unauthorized access,	• Personal Information, which must be protected under the BC *Freedom of*	Moderate harm to one or more individuals, identity theft, impact to University reputation or operations, financial loss, such as regulatory

Definition	Examples	Potential Impact of Loss
use or destruction, and could cause moderate harm if disclosed	*Information and Protection of Privacy Act* (FIPPA), including: ○ Full face photographic images ○ 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)	fines and increased credit card transaction fees
Very High Risk Information		
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

2.2 The classification of UBC Electronic 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.

3. Electronic Service Risk Classification Model

3.1 Factors to consider when assessing the risk of an Electronic Service include:

3.1.1 Reputational harm

3.1.2 Financial losses

3.1.3 Number of affected Constituents

3.1.4 Volume of High or Very High Risk Information

3.1.5 Operational impact

3.2 UBC Electronic Services are classified as follows:

Definition
Low Risk Electronic Service
Loss of confidentiality, integrity or availability in a Low Risk Electronic Service would cause minimal impact to UBC's mission, safety, finances or reputation. The incident will display one or more of the following characteristics and no characteristics of higher risk classifications: • Potential financial losses could easily be funded through departmental operating funds; • Negligible effects on UBC or departmental operations; • Affects only some or no members of one group of Constituents if confidentiality breached; or • No (one day or less) negative impact on public perception.
Medium Risk Electronic Service
Loss of confidentiality, integrity or availability in a Medium Risk Electronic Service would cause minor impact to UBC mission, safety, finances, or reputation. The incident will display one or more of the following characteristics and no characteristics of higher risk classifications: • Potential financial losses could be covered with departmental funds but would significantly impact financial position; • Normal administrative difficulties experienced; • Affects only one group of Constituents, is unlikely to impact the entire group and impacts are not significant if confidentiality breached; or • Very brief (one week to six months) negative impact on UBC public perception.
High Risk Electronic Service
Loss of confidentiality, integrity or availability in a High Risk Electronic Service would have a significant business impact to one or more portfolios, but not the whole University. The incident will display one or more of the following characteristics and no characteristics of higher risk classifications: • Potential financial losses would require funding from contingency funds, the department would have no ability to cover, but the University could cover without significant impact (e.g. $500,000 to $5 million); • Delay to accomplishing UBC objectives resulting is short term non-routine measures to mitigate; • Major impact with medium-term (six months to one year) harm to a significant membership (25% or more) of one or more Constituents, if confidentiality breached; or   ○ Significant harm to a small Constituent group; • Medium term (six months to one year) negative impact on UBC public perception; or • Non-compliance with contractual requirement to maintain availability.
Very High Risk Electronic Service
Loss of confidentiality, integrity or availability in a Very High Risk UBC Electronic Service would have a major business impact to the University. The incident will display one or more of the following characteristics: • Financial losses are major and would impact the University's ability to execute its strategic plan; • Major disruption resulting in medium term (six months to one year) non-routine measures before UBC objectives can be met; • massive impact with long-term (more than one-year) harm to most of one or more Constituents if confidentiality breached; Massive impact with long-term damage to UBC public perception;

Definition
• Impact to life safety; • Non-compliance with statutory or regulatory requirement to maintain availability; or • National security implications. These systems transact or store any of the following: • High and Very High Risk Information of most members of internal constituents (student, faculty, staff, alumni); • high volumes of research information pertaining to external constituents/research subjects; or • contractual document or intellectual property of significant sensitivity. All IT infrastructure that is critical to the operations of the University falls into this category.

4. Responsibilities

4.1 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.

4.2 The Administrative Head of Unit is responsible for ensuring completion of an inventory and classification of UBC Electronic Services under their control using the Electronic Services Risk Classification model. This must be recorded in the enterprise asset inventory system, if it is available.

4.3 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.

4.4 For UBC Electronic Services classified as Very High Risk, the Administrative Head of Unit is responsible for having documented assurance of compliance with the Information Security Standards. This is usually attained by sourcing Security Threat Risk Assessments at various stages in the information systems lifecycle (implementation, significant change, retirement).

5. Related Documents and Resources

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

BC Freedom of Information and Protection of Privacy Act (FIPPA)

What is Personal Information? [Privacy Fact Sheet]

Sample Inventory

Case Studies