University of Victoria

Information Security Policy

University Policy No: IM7800
Classification: Information Management
Approving Authority: Board of Governors
Effective Date: September 2021
Supersedes: July 2018
Last Editorial Change: December 2023
Mandated Review: September 2028

Associated Procedures:
Procedures for Responding to an Information Security Incident
Procedures for Addressing Security Vulnerabilities of Electronic University Information and Information Systems
University Information Security Classification Procedures
Procedures for Responding to the Loss or Theft of a Computing or Storage Device
Payment Card Acceptance Procedures
Procedures for the Secure Adoption and Operation of Cloud Services
Security Threat and Risk Assessment Procedures

Preamble

1.00 Information is vital to the University of Victoria (UVic) and is used in every aspect of the university's business. Without timely access to accurate information, the university would be unable to fulfil its responsibilities to internal and external stakeholders. Increasingly, the university is reliant on electronic information and the controls over information systems and devices.

2.00 With increasing reliance on electronic information and information systems comes a corresponding requirement for the security of that information. The university must be able to rely on the three key aspects of information security:

(a) confidentiality (sensitive information can be accessed only by those authorized to do so);
(b) integrity (information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version); and
(c) availability (information can be accessed when needed and in a timely manner).

3.00 The amount and type of risk that the university is ordinarily prepared to take in order to meet its objectives is described in the university's Risk Appetite Statement(s). The university must manage information security according to Risk Appetite and applicable policy. Loss of confidentiality, integrity, or availability of information can result in adverse consequences for the university.

Purpose

4.00 This policy, along with associated procedures and standards referenced below, provides guidance on how members of the university community will manage information security in accordance with other university policies, procedures, and standards designed to protect and safeguard information against unauthorized use, disclosure, modification, damage, or loss:

1) In accordance with the value and sensitivity of the resource and asset to be protected.
2) As required by the *Freedom of Information and Protection of Privacy Act* and other relevant legislation.
3) At a level congruent with the university's Risk Appetite.

Definitions

5.00 For the purposes of policy IM7800, the following definitions apply:

"administrative authority" means individuals with administrative responsibility for Units including but not limited to: Vice-Presidents, Associate Vice-Presidents, Executive Directors, Deans, Chairs, Directors, Chief Information Officer, and other Unit heads.

"information" means any electronic communication or electronic representation (i.e. digitization) of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual and includes Records.

"information security" means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability for the information they contain.

"information security standards" refer to the UVic Information Security Standards published and maintained by University Systems that apply to all UVic information systems; they are designed to protect the confidentiality, integrity, and availability of university information.

"information system" means the technologies, assets, infrastructure, equipment, and facilities owned by, explicitly controlled by, in the custody of the university, or contractually provided by a third-party that access, store, or transmit information (e.g. cloud services providers).

"**information system owner**" is the Administrative Authority responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system.

"institutional information system" means an information system that is provided by University Systems for use by the university community including, but not limited to, systems that provide infrastructure services, such as the campus network and internet connectivity, systems that manage campus reporting, student information, learning management, human resource information, financial information, and systems that

contain primary records of information such as identity and access management systems.

"provider" means technical staff, work units or external service providers/vendors who design, manage, and operate information systems (e.g. project managers, system designers, software developers, business analysts, systems analysts, application administrators, cloud tenant administrators, cloud service providers, network administrators, or system administrators).

"**risk owner**" means the Vice-President identified to oversee the management of a risk.

"security incident" means a situation where security is known or assumed to have been threatened, including but not limited to: loss of information or records confidentiality, disruption of data or system integrity, or disruption or denial of availability.

"unit" means a group of users linked by a common interest or purpose, including but not limited to: faculties, departments, divisions, schools, offices, and centres.

"university community" means:

(a) credit and non-credit students, including distance students and continuing education students;
(b) employees (faculty, librarians, and staff);
(c) any person holding a university appointment whether or not that person is an employee;
(d) post-doctoral fellows;
(e) all persons who are employed under contracts with university faculty members as the employer and who provide research or administrative services directly supporting faculty members' research activities;
(f) visiting researchers;
(g) anyone contractually required to abide by university policies;
(h) anyone volunteering with a university program or activity;
(i) members of the Board of Governors and Senate;
(j) separately incorporated organizations operating on campus; and
(k) anyone who ordinarily resides in campus because of their relationship with the university.

"user" means any member of the university community that uses or accesses information systems

Scope

6.00 This policy applies to all users and units. It applies to all UVic information, information systems, activities, and all assets owned, leased, controlled, under the custody of UVic, or contractually provided by a third-party, that are used by any user.

7.00 This policy also applies to information sharing arrangements with external parties. External service providers or parties must be bound by the relevant information-handling

aspects of this policy and associated procedures (e.g. Information Security Classification).

Policy

Statements of Intent

8.00 Protecting the university's electronic information, information systems and infrastructure is a responsibility shared by all members of the university community.

9.00 Information and information systems will be adequately protected throughout their lifecycles according to their Information Security Classification and level of acceptable risk.

10.00 Risks for information systems will be minimized. Significant new risks or changes to risk in information systems must be accepted by an appropriate Risk Owner.

11.00 To optimize system security, administrative efficacy, and best use of available university resources, it is expected that units will preferentially use institutional information systems, where available.

12.00 Where an Administrative Authority wishes to use or develop a non-institutional information system they must ensure it handles information in a manner that is compliant with all applicable legislation and policies, including IM7800 and GV0235, in consultation with the Procedural Officer(s) for the applicable policies.

13.00 Where an Administrative Authority wishes to use or develop a non-institutional information system that will interface or integrate with institutional information systems, permission must first be received from the Vice-President, Finance and Operations, in consultation with the Associate Vice-President & Chief Information Officer. The Vice-President, Finance & Operations will also consult with other executives where needed.

14.00 Users are expected to follow this information security policy, associated procedures and standards.

Roles and Responsibilities

Users

15.00 Users must:

(a) use information and information systems in a manner that protects information in accordance with UVic policy, and associated procedures, and relevant standards;
(b) agree to the policy on Acceptable Use of Electronic Information Resources (IM7200) to obtain credentials to access information systems and to continue to abide by this policy when accessing information systems;
(c) report security incidents and violations of this policy to the Information Security Office.

Providers

16.00 Providers are responsible for developing and maintaining security controls for systems within their responsibilities in accordance to university policies, procedures and standards. Providers must:

a) analyze threats, risks and adequacy of security controls in order to provide recommendations to Administrative Authorities;
b) communicate changes in security risk to Administrative Authorities;
c) at minimum follow the university information security standards, or exceed them consistent with the level of acceptable risk established by Administrative Authorities;
d) implement and document user access and privileged account controls including authorizing, renewing, retiring, and revoking access in a timely manner;
e) provide training and system documentation to users and appropriate University Systems personnel;
f) establish and test contingency plans, data back-ups, and recovery processes;
g) report security incidents to Administrative Authorities and the Information Security Office immediately upon discovery;
h) assist in the investigation and resolution of security incidents in a timely manner, preserving evidence where required; and
i) provide training and information necessary to support this policy.

Administrative Authorities

17.00 Administrative Authorities are responsible for the security of information and information systems within their unit. In some cases, they may also be defined as the information systems owner. Administrative Authorities must:

(a) identify and communicate the purpose and provider(s) of the information systems within their responsibilities to University Systems;
(b) ensure that providers develop and maintain security controls;
(c) ensure that providers fulfill their responsibilities under this policy;
(d) ensure that information is protected according to its University Information Security Classification and information security standards;
(e) ensure that security incidents are identified and resolved for the systems they manage;
(f) manage unit-specific information security risks in accordance with the university's risk management policies; and
(g) work with University Systems and Risk Owners to communicate and manage changes in risk.

Associate Vice-President University Systems and Chief Information Officer

18.00 The Associate Vice-President University Systems and Chief Information Officer (AVP & CIO) oversees the security of information systems for the university. The role of AVP & CIO will:

(a) coordinate the implementation, administration, and support of this policy;
(b) provide policies, procedures and standards;
(c) act as the Administrative Authority for institutional information systems;

(d) provide direction on compliance with the policy to university leaders and Administrative Authorities;
(e) manage cross-institutional information security risks in accordance with the university's risk management policies; and
(f) responsible for the investigation of security incidents and violations of this policy, including providing guidance and direction to Administrative Authorities and Providers during security incidents.

Chief Information Security Officer and Information Security Office

19.00 Under the direction of the CIO, the Chief Information Security Officer (CISO) leads the Information Security Office to coordinate and manage the information security program for the university. The role of CISO will:

(a) establish and maintain security objectives, strategies, and plans for the information security program;
(b) develop information security policy, procedures, standards and guidelines;
(c) create awareness about the university community's responsibilities within this policy;
(d) monitor for, initiate, assess, and respond to information security threats, risks, and exposures;
(e) support Administrative Authorities to establish acceptable levels of information security risk; and
(f) provide advice and direction to Providers in developing and maintaining security controls for information systems.

General Counsel, Chief Privacy Officer, University Secretary, and University Archivist

20.00 The General Counsel, Chief Privacy Officer and the University Secretary, in conjunction with the University Archivist, will:

(a) create awareness across the university community about members' responsibilities within this policy; and
(b) establish processes for compliance with information security policy, procedures and university information security standards through the Records Management and Protection of Privacy policies and procedures.

21.00 *Vice-President Finance and Operations*

The Vice-President Finance and Operations is responsible to oversee and enforce this policy. This authority is delegated from the Board of Governors.

Board of Governors

22.00 The Board is the authority and approval body for the university's Information Security Policy. The Board also plays a role to ensure that information security retains an appropriate focus within the organization.

Compliance

23.00 Non-compliance of this policy and its associated procedures will be reported to the Information Security Office. Users who have breached this policy, other university policies or laws may face repercussions, including loss of access to institutional

information systems, and discipline, in accordance with the relevant collective agreement and/or university policies and procedures.

24.00 The university reserves the right to rescind access to institutional information systems where necessary to protect the security of institutional information systems or to avoid further breach of a university policy or law, on an interim basis without advance notice to the user. Users whose access has been rescinded will be informed at the earliest practical opportunity of the reasons for that action.

25.00 Breaches by third parties, such as service providers and vendors, may be considered cause for the termination of the contractual arrangement with the university.

26.00 Where suspected violations of this policy involve personal information, as defined in the *Freedom of Information and Protection of Privacy Act*, the Chief Privacy Officer will be informed and asked to review and recommend appropriate action.

Review

27.00 This policy, and any subsequent recommended changes to this policy, must be approved by the Board of Governors. The Board (or a delegated authority) will review this policy for ongoing appropriateness.

Authorities and Officers

28.00 The authorities and officers for this policy are:

i. Approving Authority: Board of Governors
ii. Designated Executive Officer: Vice-President Finance and Operations
iii. Procedural Authorities: *Refer to individual procedures*
iv. Procedural Officers: *Refer to individual procedures*

Relevant Legislation

Freedom of Information and Protection of Privacy Act, RSBC 1996 c 165

Related Policies and Documents

- Acceptable Use of Electronic Information Resources Policy (IM7200)
- Enterprise Risk Management Policy (GV0225)
- Key and Access Card Control Policy (BP3125)
- Protection of Privacy Policy (GV0235)
- Purchasing Policy (FM5105)
- Records Management Policy (IM7700)
- Directory of Records
- Information Security Standards
- Technical Approval Process

University of Victoria

Procedures for Responding to an Information Security Incident

Procedural Authority: Vice-President, Finance and Operations
Procedural Officers: Chief Information Officer, General Counsel, Chief Information Security Officer
Parent Policy: Information Security Policy (IM7800)

Effective Date: September 2021
Supersedes: December 2010
Last Editorial Change:

Purpose

1.00 The purpose of this document is to set out response procedures to be followed when an information security incident occurs at the university.

Definitions

2.00 The definitions contained within the university's Information Security and Protection of Privacy policies apply to these procedures.

Examples of security incidents include, but are not limited to:

- Unauthorized use of your username and password to access university information systems, e.g. impersonating you in emails to others, downloading student information from the student information system, changing student grades or marks in the learning management system.
- Installation of unwanted or disruptive software on university computing devices, e.g. software that encrypts files and demands a ransom.
- Defacement of a public university website, or unauthorized alteration of publicly posted information.
- Disruption of access to university information systems, e.g. denial of service attack against a university online resource.

Procedures

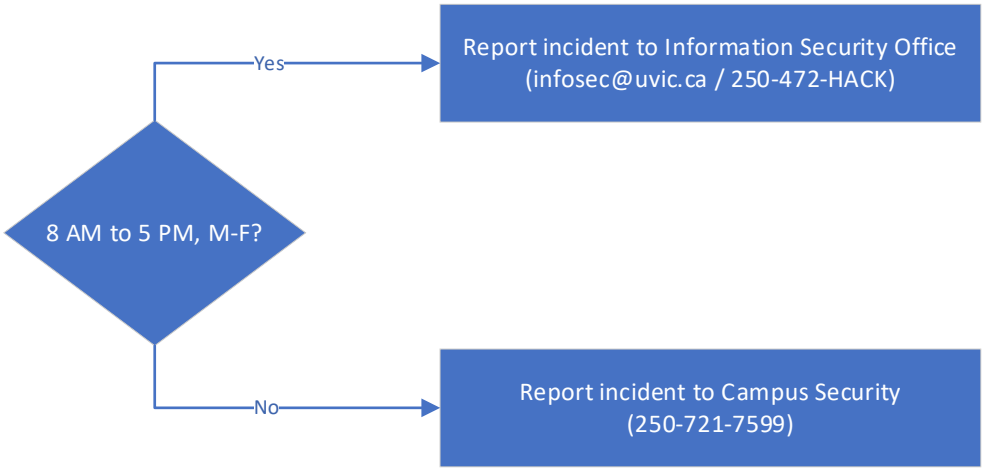
3.00 There are several stages of activity when responding to an information security incident: identification and reporting, containment, eradication, recovery, follow-up, and correction. While the stages are listed sequentially, activities from various stages may overlap depending on the nature of the incident.

4.00 It is essential to respond to information security incidents in a timely manner. This can make the difference between a major and minor incident and whether or not there is a data breach. Wherever possible, response personnel will be empowered to act quickly to reduce the impact of information security incidents.

5.00 Incidents may occur in any unit at the university. Regardless of where an incident occurs, the Information Security Office is responsible for coordinating the response and providers and administrative authorities are expected to follow the direction of the Information Security Office.

5.01 External incident response vendors may be engaged by General Counsel as required; the Information Security Office will coordinate these resources as well.

Identification and Reporting



6.00 Any member of the university community, as well as external third parties, may report information security incidents.

6.01 Information security incidents must be immediately reported to the university's Information Security Office:

a) Incidents reported to the Computer Help Desk or Desktop Support Services will be internally escalated to the Information Security Office.

b) Report incidents directly to the Information Security Office via email to infosec@uvic.ca or voicemail to 250-472-HACK (4225).

c) Outside of 8 AM to 5 PM on weekdays when the university is open, contact Campus Security via their 24-hour number: 250-721-7599.

6.02 The Information Security Office may request additional information in order to effectively respond; this information must be provided as quickly as possible.

7.00 The Information Security Office will conduct an initial assessment in order to determine the severity of the information security incident. An incident's severity will determine future actions surrounding the incident, including notification requirements or the necessity to assemble a response team or activate the university's Emergency Operations Centre (EOC).

The incident's severity will be determined based on factors such as the:
(a) sensitivity and criticality of the information or information systems involved;
(b) operational impact on the university or a unit;
(c) magnitude of the service disruption;
(d) threat potential;

(e) expanse or scope of the incident;
(f) impact to the university's reputation; or
(g) other adverse impacts on the university, individuals, or third-parties.

The severity of an incident may not be initially apparent and so actions may change at any point during the response as new information is learned.

8.00 Where and when it appears to the Chief Information Security Officer that there has been a significant information security incident, the Chief Information Security Officer will inform the Associate Vice-President University Systems & Chief Information Officer and General Counsel.

8.01 The Chief Information Officer will inform the requisite administrative authority (or designate) of the information security incident and may notify the Vice-President Finance and Operations as appropriate.

8.02 Where the information security incident does or may involve the unauthorized disclosure of personal information, the Chief Information Security Officer will inform the Chief Privacy Officer.

8.03 General Counsel will determine if external legal counsel/breach coach is required and provide direction regarding the creation and handling of legal advice related to the incident, including any reports created.

8.04 General Counsel will facilitate the use of external incident response vendors as required.

9.00 The Chief Information Security Officer may, if warranted, assemble a response team that includes the following individuals (or their designates):

(a) the Chief Information Security Officer
(b) the Manager, Information Security Office;
(c) the Associate Vice-President University Systems & Chief Information Officer; and
(d) the administrative authority responsible for the information or information systems involved.

Based on the nature of the incident, regardless of severity, the response team may also include the following individuals (or their designates):

(a) Chief Privacy Officer;
(b) Associate Vice-President Human Resources;
(c) General Counsel;
(d) Associate Vice-President Faculty Relations and Academic Administration;
(e) Executive Director, University Communications + Marketing;
(f) Director, Campus Security;
(g) Manager, Emergency Planning;
(h) Manager, Risk, Insurance & Continuity Planning;
(i) Manager, Computer Help Desk;
(j) other administrative authorities; and/or
(k) other subject matter experts.

The above individuals may be notified of the incident before their active participation is required on the response team.

10.00 For a major information security incident that may potentially disrupt the university's programs and activities, the Associate Vice-President University Systems & Chief Information Officer and General Counsel will consult the Director, Campus Security regarding the activation of the EOC.

11.00 For a major information security incident that may necessitate insurance claims or reporting, the Chief Information Security Officer will inform the Manager, Risk, Insurance & Continuity Planning.

Containment

12.00 The Chief Information Security Officer (or designate), with the cooperation of the administrative authority and/or provider responsible for the information resource, will take steps to require that requisite unit(s) makes reasonable efforts to contain the incident by, for example:

(a) stopping the unauthorized practice;
(b) recovering the information or records that were improperly collected, used, disclosed, or disposed of;
(c) shutting down affected systems;
(d) revoking access;
(e) changing computer access codes;
(f) blocking network access; or
(g) correcting weaknesses in physical security.

13.00 Where a unit is not able to take the steps recommended, a request will be submitted to the Associate Vice-President University Systems & Chief Information Officer to approve further investigation and action.

13.01 In instances where the Chief Information Security Officer (or designate) assesses that the incident is significant, and time is of the essence, the Chief Information Security Officer (or designate) may implement temporary security measures in order to mitigate any risks related to the incident until the incident has been addressed. In certain cases, such temporary security measures may be implemented prior to notifying the administrative authority or provider in the affected unit(s) in order to mitigate risks associated with the incident. In cases where action will impair the ability of the unit or person to fulfill their responsibilities, the approval of the Associate Vice-President & Chief Information Officer will be required before taking this step.

Eradication

14.00 After an information security incident has been contained, the administrative authority or provider responsible for the information or information systems involved will take action to eliminate the problem or mitigate vulnerabilities that may allow a reoccurrence of the incident and provide timely and regular reporting of their actions to the Information Security Office.

Recovery

15.00 After an information security incident has been eradicated, the administrative authority or provider responsible for the information and information systems involved will attempt to fully-restore the information systems by, for example:

(a) restoring information or information systems from backups;
(b) validating that the information is complete and accurate or that an information system is operating correctly; or
(c) performing additional monitoring.

Follow-up and Correction

16.00 Once action has been taken to mitigate the risks associated with the incident, upon the recommendation of the response team (where formed), the Chief Information Security Officer will determine whether further investigation of the incident is necessary. The response team will conduct any further investigation.

17.00 Once all investigations are complete, the response team will provide a report of the incident to the appropriate administrative authorities which may include:

(a) a summary of the incident;
(b) corrective actions taken;
(c) recommendations made for additional safeguards;
(d) follow-up actions required; and
(e) lessons learned.

Related Policies and Documents

- Information Security Policy (IM7800) and associated procedures
- Protection of Privacy Policy (GV0235) and associated procedures
- Records Management Policy (IM7700) and associated procedures

University of Victoria

Procedures for Addressing Security Vulnerabilities of Electronic University Information and Information Systems

Procedural Authority: Vice-President Finance and Operations
Procedural Officers: Chief Information Officer, General Counsel, Chief Information Security Officer
Parent Policy: Information Security Policy (IM7800)

Effective Date: September 2021
Supersedes: June 2017
Last Editorial Change:

Purpose

1.00 The purpose of these procedures is to help prevent security incidents by setting out a process to identify and mitigate potential vulnerabilities that may threaten electronic university information or information systems' security.

Definitions

2.00 The definitions contained within the university's Information Security policy (IM7800) apply to these procedures.

"vulnerability" means an identified security weakness in university information or an information system that could lead to a security incident.

Procedures

Prevention

3.00 In accordance with the university's Information Security Standards, providers are responsible for monitoring for vulnerabilities using vendor notifications or industry publications and addressing them within the specified time frames in accordance with their identified criticality. If patches are available, they must be applied within the specific time frame; if patches are not available, risk mitigation workarounds must be applied instead.

3.01 University Systems or the Information Security Office may also share vulnerability information and directions regarding remediation and providers are expected to follow these directions.

Vulnerability Identification and Reporting

4.00 In accordance with the Information Security policy (IM7800), the university monitors its network and connected information systems for potential security exposures and takes pre-emptive action to prevent security incidents before such incidents occur. This includes conducting assessments of electronic information and information systems to identify potential vulnerabilities that may threaten such resources. The monitoring or assessment may unintentionally reveal personal information.

4.01 Potential vulnerabilities may be:

(a) recognized by the Information Security Office as part of regular network and information system monitoring, assessment, or maintenance;
(b) communicated by a vendor or trusted third party;
(c) reported to the Information Security Office when a provider, administrative authority (or designate), or other individual becomes aware of a vulnerability;
(d) reported as part of the Information Security Office's Vulnerability Disclosure process.

Preliminary Assessment

5.00 Where the Information Security Office becomes aware of a vulnerability to information or in an information system, the Information Security Office will conduct an initial assessment to determine the potential impact of the vulnerability.

5.01 The potential impact of the vulnerability will be assessed based on factors including but not limited to the:

(a) sensitivity and criticality of the information or information systems involved;
(b) likelihood of the vulnerability causing a security incident;
(c) operational impact to the university or a unit;
(d) operational impact on other information or information systems;
(e) threat potential; and
(f) other potential impacts on the university, individuals, or third parties.

Notification and Implementation of Corrective Actions

6.00 Where the Information Security Office reasonably believes that a vulnerability threatens university information or an information system, the Information Security Office will create a report with recommendations detailing actions and timelines required for addressing the vulnerability and will provide the report to the Administrative Authority responsible for the Unit and/or Provider of the vulnerable system(s) and to the Chief Information Security Officer.

6.01 The Administrative Authority or Provider of the vulnerable system(s) is responsible for reporting its response to and implementation of the recommended actions (or reasonable alternate actions) to the Chief Information Security Officer and the Information Security Office.

i. Failure to acknowledge receipt of the report and submit an acceptable response plan may lead to escalation up to and including the Vice-President responsible for the unit.

6.02 In instances where the Chief Information Security Officer (or designate) assesses that the vulnerability is significant, and time is of the essence, the Chief Information Security Officer (or designate) may implement temporary security measures in order to mitigate any risks related to the vulnerability until the vulnerability has been addressed. In certain cases, such temporary security measures may be implemented prior to notifying the Administrative Authority or Provider of the vulnerable system(s) in order to mitigate risks associated with the vulnerability. In cases where action will impair the ability of the unit or person to

fulfill their responsibilities, the approval of the Chief Information Officer will be required before taking this step.

7.00 Where the Chief Information Security Officer (or designate) assesses that the vulnerability is significant and remediation actions taken by the Administrative Authority or Provider are not commencing in a timely or appropriate manner, the Chief Information Security Officer (or designate) may take temporary security measures to mitigate any risks until the vulnerability has been addressed. Such measures may include but are not limited to: temporarily shutting down affected systems, or blocking or revoking access.

Follow-up and Correction

8.00 Once action has been taken to mitigate the risks associated with the vulnerability, the Chief Information Security Officer (or designate) will determine whether further investigation or monitoring of the vulnerability is necessary, and will provide a report to the Administrative Authority and/or Provider of the vulnerable system(s).

Related Policies and Documents

- Information Security Policy (IM7800) and associated procedures
- Protection of Privacy Policy (GV0235) and associated procedures
- Records Management Policy (IM7700) and associated procedures

University of Victoria

University Information Security Classification Procedures

Procedural Authority: Vice-President Finance and Operations
Procedural Officers: Chief Information Officer, Chief Privacy Officer, General Counsel, Chief Information Security Officer
Parent Policies: Information Security Policy (IM7800)
Protection of Privacy Policy (GV0235)

Effective Date: September 2021
Supersedes: January 2015
Last Editorial Change:

Purpose

1.00 The purpose of these procedures is to set out the minimum standards necessary for classifying various types of university information resources so that reasonable security arrangements can be applied to such information.

Definitions

2.00 The definitions contained within the university's Information Security (IM7800) and Protection of Privacy (GV0235) policies apply to these procedures:

Note: Refer to the Procedures for the Management of University Records and the Directory of Records for information on the functional classification of university records. Refer to the Procedures for the Access to and Correction of Personal Information for information regarding freedom of information access requests.

See section 8.00 for definitions of security classification levels.

Procedures

Assigning an Information Security Classification Level

3.00 Information resources must be assigned a security classification by the Administrative Authority at the level appropriate for that resource, in accordance with the classification levels set out in section 8.00.

3.01 The security classification level of the information resource establishes the extent and type of security arrangements that must be implemented in order to protect the information resource.

3.02 Prior to assigning a security classification level, units must be aware of relevant legislative requirements and regulatory obligations, and relevant university policies, procedures, and standards. Units may also refer to industry standards and best practices for further direction where applicable if they meet or exceed university standards.

4.00 Administrative authorities must classify and manage the information resources for which they are responsible based on a reasonable understanding of the overall value of the information resource. Where appropriate, administrative authorities should collaborate with providers and University Archives to classify and manage the information resources for which they are responsible.

5.00 Administrative authorities must require that users in their units manage information resources according to the assigned security classification.

6.00 Security classification levels are applied to broad information types or categories, rather than individual records.

7.00 Where it is unclear which security classification level is most appropriate or when dealing with large volumes of information, units should employ the highest appropriate classification level.

7.01 Where an information system or record contains information that is classified as public and information classified at a higher level, the combined information must be managed at the higher confidentiality level.

7.02 In deciding which security classification level is most appropriate, units will take into account the volume of information and should consider employing a higher classification level for large volumes of information. An increase in risk due to volume may necessitate using a higher security classification level.

Information Classification Levels

8.00 University information resources are classified according to the classification levels in the following chart.

	Highly Confidential	Confidential	Internal	Public
Definition	Information resource is so sensitive or critical that it is entitled to extraordinary protections, as defined in section 9.00.	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 who have explicit authorization to review such information, even within a workgroup or unit.	Information that is intended for use within the university or within a specific workgroup, 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 information owner or administrative authority or through some other valid authority such as legislation or policy.
Legal Requirement	Protection of information where it is required by law or regulation (e.g. FIPPA or PCI-DSS), or as determined by contractual obligation.	The university has a contractual or legal obligation to protect the information.	The university has a contractual obligation to protect the information.	Information may be mandated by legislation (e.g. FIPPA) to be public information.
Reputational Risk	Critical loss of trust/credibility. Significant media attention. Business unit will be subject to special training and processes.	Significant loss of trust/credibility. Guaranteed to generate media attention and increased scrutiny.	Potential for lost trust/credibility, and financial liability for breach of contract. May generate some media attention and result in increased scrutiny.	No impact on reputation.
Operational Risk	Risk will render the business unit unable to achieve its overall objectives or mandate.	Significant impact on business unit's ability to achieve its objectives.	Moderately impacts business unit's ability to achieve its objectives.	Little or no impact on the business unit's ability to achieve its objectives.
Financial Risk	Major revenue loss, or impact on business unit budget, including research funding, or fines.	Significant revenue loss, or impact on business unit budget, including research funding, or fines.	Moderate negative financial impact for the business unit.	Impact is within normal operating budget margin fluctuations.
Disclosure Risk	Highly adverse negative impact on the university, individuals, or affiliates, including identity theft.	Moderately adverse negative impact on the university, individuals, or affiliates, including identity theft.	Possible adverse impact on the university, individuals, or affiliates.	Disclosure of public information requires no further authorization and may be freely disseminated without potential harm to the university or its affiliates.

8.01 **Prohibited Information:** In addition to the above classification levels, certain information may be deemed by industry regulations, legislation, or other mechanism to be prohibited. Such information may not be collected or stored by the university in any form.

Security Arrangements for Classification

9.00 After an information security classification has been applied, reasonable security arrangements are required that correspond to the assigned classification level. The following table sets out appropriate safeguards for each level of information.

	Highly Confidential	Confidential	Internal	Public
Access	• Access is limited to specific named individuals or positions. • Principles of least-privilege and need-to-know must be applied • Access must be revoked immediately when users leave the university or the custodial unit.	• Access is limited to individuals in a specific function, group, or role. • Principles of least-privilege and need-to-know must be applied • Access must be revoked as soon as reasonably possible when users leave the university or the custodial unit.	• Access is limited to employees and other authorized users for business-related purposes. • Access must be revoked as soon as reasonably possible when users leave the university or the custodial unit.	• No access restrictions
Transmission	• Encryption required for all networks (e.g. wireless, Internet, and internal networks). • Avoid emailing if at all possible use secure file sharing methods instead (e.g. departmental shared drive, UVic SharePoint site, UVic Teams site); if email is unavoidable, must use uvic.ca email system and put data inside password protected email attachments, share the password via a secure secondary channel (e.g. phone call). • Double envelope mailings for hardcopy records.	• Encryption required for public networks (e.g. wireless, Internet). • Encryption strongly recommended on trusted, internal networks. • If emailing, must use uvic.ca email system and put data inside password protected email attachments. • If emailing, must use uvic.ca email system and password protect attachments, share the password via a secure secondary channel (e.g. phone call). • Clearly marked "confidential" on sealed mailings.	• Encryption strongly recommended on public networks (e.g. wireless, Internet). • If emailing, must use uvic.ca email system.	• No special handling required.
Storage	• Stored within a controlled-access system (e.g., password protected file or file system, locked file cabinet, alarmed area). Additional controls implemented as necessary to comply with relevant legislation or other requirements. • Encryption mandatory in all environments. • Implement "clean desk" policy.	• Stored within a controlled-access system (e.g., password protected file or file system, locked file cabinet, alarmed area). • Encryption mandatory on mobile devices and workstations, and strongly-recommended in all environments. • Implement "clean desk" policy.	• Stored within a controlled-access system (e.g., password protected file or file system, locked file cabinet). • Encryption strongly recommended in all environments.	• Stored within a system that ensures only authorized personnel can alter the information.
Destruction	• Shredded or securely erased in accordance with the university's Guidelines for the Secure Destruction of Information	• Shredded or securely erased in accordance with the university's Guidelines for the Secure Destruction of Information	• Shredded or erased in accordance with the university's Guidelines for the Secure Destruction of Information	• Recycle

Relevant Legislation

Freedom of Information and Protection of Privacy Act, RSBC 1996 c 165

Related Policies and Documents

- Information Security Policy (IM7800) and associated procedures
- Protection of Privacy Policy (GV0235) and associated procedures
- Records Management Policy (IM7700) and associated procedures
- Acceptable Use of Electronic Information Resources (IM7200) and associated procedures

---

Appendix A: Information Classification Requirements

The following chart provides examples of the types of information and their required security classification.

	Information
Public	• Annual reports • Advertising and media releases • Product and service information • Employee directory listings • Academic calendar • Published research presentations or papers • Job postings • Training manuals • Open-session Board and Senate minutes • Name of degree, diploma, and certificate recipients • Campus maps
Internal	• Budget information • Personal pager or cell phone numbers • Select unit procedures • Student number (V-number) • Student grades (including test scores, assignments, and class grades) • Employee V-number
Confidential	*Enrolled and Prospective Student Data* • Social Insurance Number • Driver's Licence Number • Student financials (bank accounts, wire transfers, payment history, financial aid/grants) • Biometric identifiers, including finger and voice prints, and full face images • Personal vehicle information (serial numbers, licence plate number) • Access device numbers (ISO number, building access code, keys, etc.) • Reference letters • Information protected by non-disclosure agreements • Any other unique identifying number, characteristic, or codes • Payment guarantor's and beneficiary information • Student contact or class lists • Enrolment status of an individual • Biometric identifiers, including finger, face, and voice prints, and full face images *Employee Information* • Social Insurance Number • Personnel files • Personal vehicle information (serial numbers, licence plate number) • Accounting information (tax records, employee payroll, staff loans, etc.)

	• Access device numbers (ISO number, building access code, keys, etc.) • Biometric identifiers, including finger, face, and voice prints, and full face images • Information protected by non-disclosure agreements • Personal financial information, including non-UVic income level and sources • Insurance benefit, payment guarantor's, and beneficiary information • Pension records • Employee demographic information • Any other unique identifying number, characteristic, or code • Home/personal address, phone number, cell number, email address *Donor/Alumni Information* • Donor's name • Social Insurance Number • Personal financial information • Donor profile (personal & family history) • Bank account numbers, amount donated • Telephone/fax numbers, email address • Information protected by non-disclosure agreements • Any other unique identifying number, characteristic, or code *Research Information* • Research information (Granting Agency Agreements, other IRB Governance) • Sensitive research data *Business/Vendor Data* • Contract information (between UVic and a third party) • Access device numbers (building access code, etc.) • Biometric identifiers • Certificate/licence numbers, device IDs and serial numbers, email, URLs, IP addresses *Other Institutional Data* • Confidential information in contracts • Physical plant detail • Critical infrastructure detail • User account passwords
Highly-Confidential	• Legal suits • Closed or *in camera* Board of Governors or Senate documents • Academic concessions • Appeals and grievances • Criminal records checks • Health, disability, or counselling information • Harassment and discrimination reports • Authentication credentials • Personally identifiable research information

Prohibited	*Credit Card Data / Payment Card Industry Data Security Standard (PCI DSS) (when taken as part of a financial transaction)* • Service code • ISO number • CVC2, CVV2, or CID value • PIN or PIN block • Contents of a credit card's magnetic stripe (specifically "Track 2" data)

University of Victoria

Procedures for Responding to the Loss or Theft of a Computing or Storage Device

Procedural Authorities: Vice-President Finance and Operations; General Counsel
Procedural Officer: Chief Information Officer; Chief Privacy Officer; Chief Information Security Officer
Parent Policies: Information Security Policy (IM7800)
Protection of Privacy Policy (GV0235)
Records Management Policy (IM7700)

Effective Date: September 2021

Supersedes: December 2010

Last Editorial Change:

Purpose

1.00 The purpose of this document is to set out response procedures in the event of the loss or theft of a university computing or storage device in order to protect the information contained on the device or storage.

Definitions

2.00 The definitions contained within the university's Protection of Privacy (GV0235) and Information Security (IM7800) policies apply to these procedures.

"computing device" means any device that provides computing or information storage and retrieval including but not limited to: computers, tablets, smart phones, and media including flash drives, compact disks (CD), digital video disks (DVD), and portable hard drives.

Procedures

User Responsibility

3.00 Users of university computing devices are expected to make reasonable security arrangements to protect such devices from loss or theft and to protect information stored on such devices.

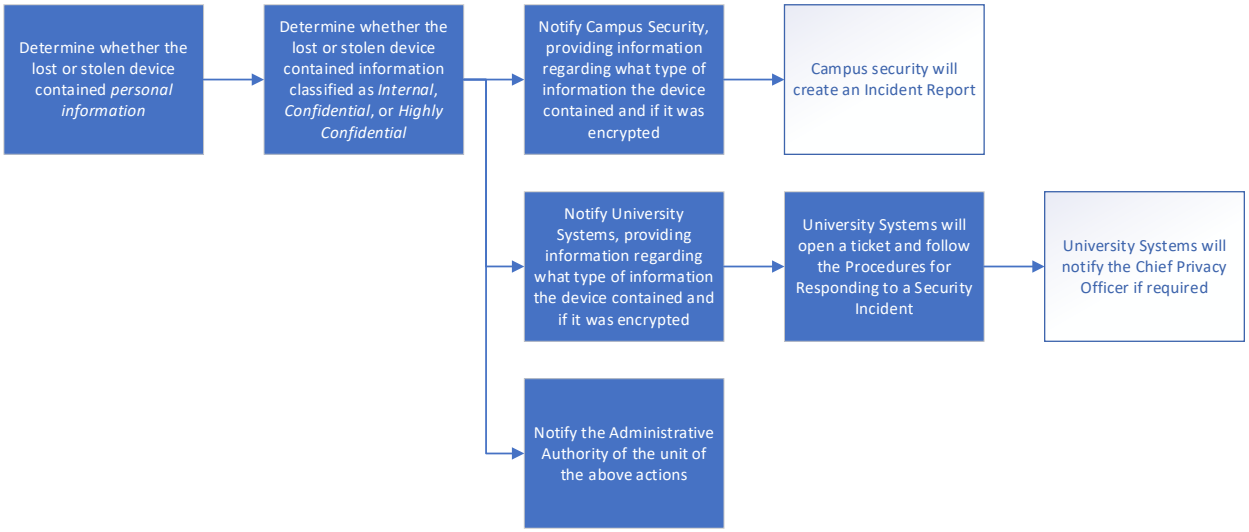
Identification and Reporting

4.00 Loss or theft of a university computing device must be immediately reported to Campus Security, University Systems, and to the unit's administrative authority.

4.01 When reporting the loss or theft, users are expected to inform Campus Security and University Systems whether the computing device:

i. contains personal information, or information classified as Internal, Confidential, or Highly Confidential under the university's Information Security Classification procedure; and
ii. is encrypted according to the university's Information Security Standards.

5.00 Campus Security will conduct an initial assessment and create an incident report.



6.00 Campus Security will inform the Information Security Office in a timely manner if the lost or stolen computing device contains:

(a) personal information; or
(b) Internal, Confidential, or Highly-Confidential information (as defined in the University Information Security Classification procedures)

so that the Information Security Office can quickly respond (as defined in the Procedures for Responding to an Information Security Incident).

7.00 Where the Information Security Office confirms that the lost or stolen computing device contains personal information, the Information Security Office shall immediately contact the Chief Privacy Officer.

Response

8.00 In cases where personal information is contained on a lost or stolen computing device, the Chief Privacy Officer, where warranted, will follow the Procedures for Responding to a Privacy Incident or Privacy Breach.

9.00 Where the information contained on the computing device is non-personal and Internal, Confidential, or Highly Confidential, the Information Security Office, where warranted, will follow the Procedures for Responding to an Information Security Incident.

Related Policies and Documents

- Information Security Policy (IM7800) and associated procedures
- Protection of Privacy Policy (GV0235) and associated procedures
- Records Management Policy (IM7700) and associated procedures

University of Victoria

Payment Card Acceptance Procedures

Procedural Authority: Vice-President Finance and Operations
Procedural Officer: Executive Director, Financial Services
Parent Policy: Information Security Policy (IM7800)

Effective Date: September 2021
Supersedes: June 2012
Last Editorial Change:

Purpose

1.00 The acceptance of payment cards provides a convenient way to process the sale of certain goods and services at the University of Victoria. Card acceptance also presents security and privacy risks that must be understood by all units accepting payment cards.

2.00 The Payment Card Industry (PCI) has established a rigorous set of security standards for the collection, storage, and transmission of cardholder data designed to provide for the security of data by protecting the privacy of personal information and safeguarding the cardholder's bank accounts and assets. All university units must meet the requirements for security.

2.01 Implementation of PCI security controls is also part of the university's Information Security Standards.

3.00 The purpose of this procedure is to establish responsibilities and expectations of university units who accept payment cards.

Definitions

4.00 For the purposes of these procedures, the following definitions apply.

"cardholder" means an individual with a payment card.

"merchant" means a unit that has applied for and been assigned an account(s) with the university's payment processor for the processing of payment card transactions.

"payment card" means a credit card, debit card, and other media that is presented by individuals for the purpose of making payments.

"payment processor" means the third party service provider that Financial Services has engaged to process payment card transactions on behalf of university merchants.

"PCI-DSS" means Payment Card Industry-Data Security Standards, which were created by major credit card companies to safeguard cardholder information. Visa, Mastercard, American Express, and other credit card associations mandate that merchants and

service providers meet certain minimum standards for security when they accept, process, transmit, and store cardholder data. Merchants are required to demonstrate compliance on a periodic basis.

"unit" means academic or administrative areas at the university, including but not limited to: faculties, departments, divisions, offices, schools, centres, and other related agencies, and the University Club of Victoria.

Scope

5.00 These procedures apply to all units which process university payment card transactions in any form and which may include:

(a) websites (eCommerce);
(b) PIN entry devices (PEDs);
(c) departmental information systems; and
(d) manual entry by staff from information provided by cardholders (fax, telephone, forms).

Procedures

6.00 The processing of payment card transactions must be carried out using the university's approved third party payment processor. Units may not enter into separate banking and/or payment processing arrangements without the approval of Financial Services.

7.00 All applications for merchant accounts are to be submitted to Financial Services.

8.00 Units looking to implement new systems or replace existing systems that will process payment cards or exchange information with systems that process payment cards must consult with Financial Services (Director, Treasury Services) and University Systems prior to proceeding to ensure these systems comply with standards required by our payment card processing agreements.

8.01 Systems that do not comply with required standards will not be permitted to process payment cards until they are brought into compliance and approved by Financial Services (Director, Treasury Services)

9.00 Units that process payment card transactions must implement and maintain PCI-DSS compliant processes and procedures identified by Financial Services and University Systems, at the expense of the unit.

10.00 Units must implement mechanisms, based on recommendations from University Systems and compliant with PCI requirements and security standards, to manage how cardholder data is securely received, stored, and transmitted and protected from unauthorized access. Cardholder data must not be transmitted by email, voicemail, or end-user messaging technologies, as these methods are not secure. PIN entry devices (PEDs) must be stored in a secure location.

10.01 Online payment forms should include mechanisms to reduce the probability of supporting fraudulent activities such as unauthorized third parties testing the validity of stolen payment card information.

11.00 Units are responsible for safeguarding the confidentiality of cardholder data and personal information relating to the sale or purchase of goods or services, and for ensuring compliance with information privacy legislation and the university Protection of Privacy Policy.

12.00 Hardcopy and electronic information collected about cardholders must be maintained in a secure manner and access must be restricted to individuals who have a valid business need to know.

13.00 The collection of cardholder data should be kept to a minimum. Data such as the primary account number (PAN), card validation codes, and personal identification numbers (PIN) must never be stored.

14.00 Information collected about cardholders, including payment information, must only be used for the purpose for which it was given.

15.00 Units are responsible for retaining appropriate transaction records for audit purposes for a period of seven years. For the retention rule for accounts receivable, see Directory of Records FM155-20.

16.00 Units with an active merchant account may be subject to periodic security audits (internal or external), at the expense of the department. Financial Services is responsible for engaging third party vendors to provide PCI-DSS compliance services.

17.00 Units found to have inadequate security (non PCI-DSS compliant) may have their merchant account privileges suspended by the Vice-President Finance and Operations in accordance with the Procedures for Addressing Security Vulnerabilities of Electronic University Information and Information Systems.

18.00 Units must fully comply with the terms of the merchant agreement between the university and its payment processor. Units may not process payment card transactions for another merchant, person, or entity. Any questions regarding the terms of the university merchant agreement should be directed to Financial Services.

19.00 Merchants are responsible for developing training materials and training their employees on an ongoing basis as per current PCI standard requirements.

Relevant Legislation

Freedom of Information and Protection of Privacy Act, RSBC 1996 c 165
Personal Information Protection Act, SBC 2003 c 63

Related Policies and Documents

- Signing Authority Policy (FM5100)
- Information Security Policy (IM7800)
- Protection of Privacy Policy (GV0235)
- Federal Department of Finance – Code of Conduct for the Credit and Debit Card Industry in Canada
- Payment Card Industry Data Security Standards
- Global Payments Merchant Agreement

University of Victoria

Procedures for the Secure Adoption and Operation of Cloud Services

Procedural Authority: Vice-President Finance and Operations
Procedural Officers: Chief Information Officer; Chief Information Security Officer
Parent Policy: Information Security Policy (IM7800)

Effective Date: September 2021
Supersedes: New
Last Editorial Change:

Purpose

1.00 The purpose of this procedure is to describe the process that must be followed whenever a unit wishes to use a cloud service provider.

2.00 When university information is provided to a third party, the university relies on their attestations that they will handle university data appropriately. This is to both minimize the risk of a security incident and to be able to assure the campus community that the transfer of information complies with the requirements of relevant legislation and university policies.

3.00 If a third party is unwilling to provide attestations to the university's satisfaction, the residual risks must be reviewed and approved by the appropriate vice-president.

Definitions

4.00 The definitions contained within the university's Information Security (IM7800) policy apply to these procedures.

Procedures

User Responsibility

5.00 The administrative authority of the unit that wishes to transfer custody of information to a cloud service provider is responsible for determining the information security classification of this information.

5.01 Note that even information classified as "public" must be protected to ensure it cannot be altered by unauthorized individuals.

6.00 Administrative authorities must complete a Privacy Impact Assessment in consultation with the Chief Privacy Officer and a Security Risk and Threat Assessment in consultation with Systems before moving information to a cloud service provider.

7.00 The administrative authority of the unit that wishes to transfer custody of information to a cloud service provider is responsible for ensuring that the contract with the cloud service provider contains the Cloud Security Schedule.

7.01 If the cloud service provider requests revisions to the Cloud Security Schedule, the administrative authority must ensure that University Systems

reviews proposed changes or alternative contractual language to mitigate information security risks.

7.02 If information security risks cannot be fully mitigated to University Systems' satisfaction, the Chief Information Security Officer will draft a Risk Memo that will document residual risks and must be reviewed and approved by the appropriate vice-president before the contract can be signed.

8.00 Cloud service implementations at UVic must meet or exceed UVic information security standards for cloud security. Certifications of compliance with or assessments against a set of accepted cloud security standards (e.g. ISO 27017, ISO 27018, NIST 800-53, CSA Cloud Control Matrix Level 2, FedRAMP Moderate, Government of Canada PBMM Security Control Profile) are preferred.

Related Policies and Documents

- Purchasing Services Policy (FM5105)
- Protection of Privacy Policy (GV0235)
- Records Management Policy (IM7700)
- Information Security Policy (IM7800)

University of Victoria

Security Threat and Risk Assessment Procedures

Procedural Authority: Vice-President Finance and Operations
Procedural Officers: Chief Information Officer; Chief Information Security Officer

Effective Date: September 2021
Supersedes: New

Last Editorial Change:

Parent Policy: Information Security Policy (IM7800)

Purpose

1.00 The purpose of this procedure is to describe the process that must be followed when implementing a new information system or making a substantial change, e.g. upgrade, to an existing information system that will:

(a) handle information classified as confidential or highly confidential, or
(b) interface or integrate with an institutional information system

in order to assess and mitigate information security risks before the system is used to handle university information. New may mean new information system to the university, new use of an existing information system by a unit, or new use of an existing information system by new unit.

Definitions

The definitions contained within the university's Information Security (IM7800) policy apply to these procedures.

"security threat and risk assessment" (STRA) means the overall activity of identifying, assessing, and reporting security risks for an information system; they are a snapshot in time and raise the system security risks in an organization to a level at which risk-based decisions can occur effectively; and they document risk ratings and planned treatments.

Procedures

2.00 A STRA can be requested at any time but must be completed for new or significantly modified information systems during planning, development, and implementation.

3.00 A review and updated STRA must be conducted throughout the life of an existing information system for any significant or material change that would affect the security and must include any previously identified risk.

3.01 A STRA should be reviewed and updated prior to contract renewal of an existing system.

4.00 A review schedule must be maintained to ensure that STRAs are periodically conducted throughout the life of an information system.

5.00 A simple or a comprehensive STRA may be used depending on the appropriateness commensurate to the information system being accessed with the goal of achieving reasonable security.

6.00 Administrative Authorities and Providers are responsible for ensuring STRAs are conducted for information systems under their custody or control and updated as required per 4.00. The Information Security Office can guide or, when requested and subject to resource availability, conduct the STRA and make recommendations.

> The Province of British Columbia has a Security and Risk Assessment process that can be a good guide for great public sector entities to model around.

7.00 To determine the reasonableness of an information system's security, each risk must consider the likelihood which a threat may leverage a weakness, the potential impact, and acknowledge what this could mean to the university (scope of impact).

8.00 For each risk identified, a planned treatment or acceptance must be documented. Risk treatment or acceptance will be conducted as appropriate in accordance with this policy and other university policies (e.g. Enterprise Risk Management Policy GV0225).