September 2021
July 2018
December 2023
September 2028

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

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)

aspects of this policy

Providers

16.00 Providers are responsible for developing and maintaining security controls for 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;

information s

Procedures for Responding to an Information Security Incident

Procedural Authority: Vice-President, Finance and Operations	Effective Date: September 2021
Procedural Officers: Chief Information Officer, General Counsel, Chief Information Security Officer	Supersedes: December 2010
Parent Policy: Information Security Policy (IM7800)	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 2.6 (e)1.2 (r)-1.7 (v)-5 (i)-2.2 (c)12.3 (e)1.3 ( )0.7 (at)-6 (t)-5.9 (ac)1.5 (P Tw

5.01

(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 sign 23 >>BDC -0.002 Tc 0.Tv13 (t)(an)(

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 VicePresident 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 VicePresident 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 VicePresident & Chief Information Officer will be required before taking this step.

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) correc3 (0)0.5 (0)]m90 1 Tf -0.005 T7 n [(co)-5.5 (r)-3.7 (r)-3.7 (e)-0.8 (-3.7 (r)-3.7 (e)-0.8 (-3.7 (reAf -

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, ad ministrative authority (or designate), or other individual becomes aware of a vulnerability;
(d) reported as part of the Information Security Office's Vulnerability Disclosure process.

Preliminar38/MCID 96 >>BDC -0.00a.6 (l)0]TJ EMC]TJ Eli

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

University Information Security Classification Procedures

Procedural Authority: Vice-President Finance and Operations
Procedural Officers: Chief Information Officer, Chief Privacy Officer, General Counsel, Chief Infos:

4.00

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 PCIDSS), 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 p rohibited. Such information may not be collected or

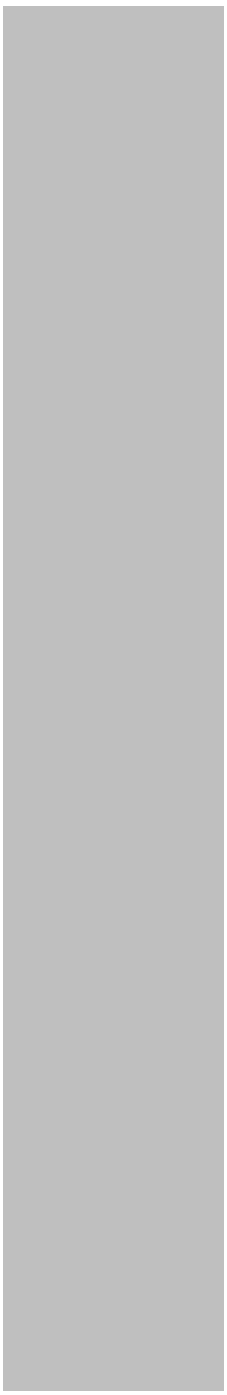
Relevant Legislation

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

---



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)

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

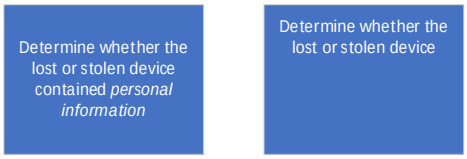
Procedural Authorities: Vice-President Finance and Operations; General Counsel	Effective Date: September 2021
Procedural Officer: Chief Information Officer; Chief Privacy Officer; Chief Information Security Officer	Supersedes: December 2010
Parent Policies: Information Security Policy (IM7800) Protection of Privacy Policy (GV0235) Records Management Policy (IM7700)	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 shall apply.


Determine whether the lost or stolen device contained *personal information*
Determine whether the lost or stolen device

Payment Card Acceptance Procedures

Procedural Authority: Vice-President Finance and Operations
Effective Date: September 2021
Procedural Officer: Executive Director, Financial Services
Parent Policy: Information Security Policy (IM7800)

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.

"u nit " 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.

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

Procedures for the Secure Adoption and Operation of Cloud Services

Procedural Authority: Vice-President Finance and Operations
Effective Date:
Procedural Officers: Chief Information Officer; Chief Information Security Officer Diat-11 89 (0-62<3ui-0J 2 10-9 6e)ft7 (5.9ii7 (5.9o--.3 62 10-9 6e)22208 (rsTJ61 0
Parent Policy : Information Security Policy (IM7800)

f i uhroP r P P h

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) meansthe 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 STRAcan be requested at any

5.00