**INFORMATION SECURITY POLICY**

**University Policy No:** IM7800
**Classification:** Information Management
**Approving Authority:** Board of Governors
**Effective date:** July, 2018
**Supersedes:** January, 2010
**Last Editorial change:**
**Mandated review:** January, 2017

**Associated Procedures:**
Procedures for Responding to an Information Security Incident
Procedures for Addressing Security Vulnerabilities of University Electronic Information Resources and Information Systems
University Information Security Classification Procedures
Procedures for Responding to the Loss or Theft of a Mobile Computing Device
Payment Card Acceptance Procedures
Guidelines for the Secure Destruction and Deletion of University Records and Information

---

## PURPOSE

1.00 The purpose of this policy is to define authorities, responsibilities, and accountabilities for Information Resources and Information Systems security.

## DEFINITIONS

2.00 **Administrative Authority** means individuals with administrative responsibility for units (e.g., Vice-Presidents, Chief Information Officer, Executive Directors, Deans, Chairs, Directors, and other unit heads) and individuals with functional stewardship of university Information Resources.

3.00 **Information Security Office** means a unit within University Systems that comprises university employees responsible for coordinating and managing the security of university Information Resources.

4.00 **Information System** means the people, processes, organization, technologies, equipment, and facilities that collect, process, store, display, transmit, and disseminate information.

5.00 **Provider** means individuals who design, manage, and operate university electronic Information Resources (e.g., project managers, system designers, application programmers, or system administrators).

6.00 **Unit** means a group of Users, linked by a common interest or purpose, including but not limited to, faculties, departments, divisions, schools, and centres.

7.00 **User** means any individual or Unit that uses or accesses university Information Resources.

8.00 **Information Resources** means assets and infrastructure owned by, explicitly controlled by, or in the custody of the university including but not limited to data, records, electronic services, network services, software, computers, and Information Systems.

9.00 **Security Incident** means any adverse event whereby some aspect of information security could be threatened, including but not limited to: loss of data or records confidentiality, disruption of data or system integrity, or disruption or denial of availability.

10.00 **University Community** members include:

- all employees and registered students of the university;
- any person holding a university appointment whether or not that person is an employee;
- post-doctoral fellows;
- separately incorporated organizations operating on campus;
- organizations and individuals required by contract to comply with university policies and procedures;
- members of the Board of Governors; and
- anyone residing on campus.

11.00 **Records** means documents created or received, and retained in the day-to-day operations of business. This includes, but is not limited to, documents, maps, drawings, photographs, letters, vouchers, papers, and any other thing on which information is recorded or stored by graphic, electronic, mechanical, or other means, but does not include a computer program or any other mechanism that produces records.

**SCOPE**

12.00 This policy applies to all University Community members. It applies to all Information Resources in the custody or under the control of the university regardless of physical location.

13.00 This policy applies to information recorded or stored by electronic, paper, or other means.

**POLICY**

14.00 Reasonable security arrangements for Information Resources are necessary to achieve the university's commitment to the protection of privacy and compliance with the *Freedom of Information and Protection of Privacy Act* and other relevant legislation.

15.00 The university shall manage information security in accordance with university policies and procedures to ensure the confidentiality, integrity, and availability of information. This will be performed in accordance to the value and sensitivity of the resource and asset to be protected.

16.00 The university is committed to creating a secure yet open computing environment in which the University Community can teach, learn, conduct research, and perform administrative functions. In order to do this, the university will protect Information Resources and Information Systems from risks such as unauthorized creation, collection, access, use, disclosure, disruption, modification, or destruction.

Guiding Principles

17.00 The university's Information Security program is guided by the following principles:

(a) Proactive: The university will take pre-emptive action to prevent Security Incidents before they happen.

(b) Monitor: The university will electronically monitor the network and connected Information Systems for potential security exposures and balance the monitoring with privacy requirements.

(c) Standards: The university will establish and continuously evaluate and improve information security procedures, standards, and guidelines.

(d) Risk: Risk exposure will be balanced with the cost of risk mitigation when assessing security choices.

(e) Institutional consistency: The Information Security Office will implement consistent institution-wide standards for electronic Information Resources.

(f) Audit: Internal Audit will provide independent ethics and effectiveness guidance for security management process.

(g) Authentication: Security enforcement applies to authentication processes and authorized role access.

(h) Universality: Each university system User is responsible for applying the security policy.

(i) Better practices: The university will implement industry-wide security better practices where appropriate.

(j) Defense-in-depth: The university will implement multiple levels of information security defense.

(k) Education: Education of system Users about security principles and the application of these principles are critical to the success of the security policy.

(l) Respond: The university will respond with corrective action to security incidents where appropriate.

Roles and Responsibilities

18.00 Each member of the University Community will make reasonable security arrangements and protect Information Resources for which the member is responsible.

19.00 The Chief Information Officer oversees the campus-wide security of electronic Information Resources and the infrastructure necessary to support the functional processes and activities of Administrative Authorities. Administrative Authorities manage the security related to the functional use of Information Systems specific to their Units. The Chief Information Officer and Administrative Authorities will work collaboratively to establish specific distinctions in information security authority where there may be the potential for overlap.

20.00 Under the direction of the Chief Information Officer, the Information Security Office is responsible for overall coordination and management of the Information Security program for the university.

21.00 The Chief Information Officer in relation to electronic Information Resources and within the role outlined in section 19.00 above:

- sets university-wide security objectives and strategies;
- develops information security policy and procedures, and provides standards and guidelines to ensure reasonable security arrangements;
- creates awareness across the University Community about members' responsibilities within this policy;
- ensures the processes and resources for monitoring, compliance, protection, detection, and correction are in place;
- identifies the Information Resources for the university;
- defines the purpose and function of the Information Resources and ensures that requisite education and documentation are provided to the university;
- establishes acceptable levels of security risk for the Information Resources by assessing factors including but not limited to the:
    - sensitivity of the Information Resources;
    - criticality of the Information Resources to the continuing operation of the university;
    - impact of security issues created at the university that may affect other organizations related to the university;
    - likelihood that an Information Resource could be used as a platform for inappropriate acts;
    - limits of available technologies, programmatic needs, cost, and staff support; and
- ensures that reasonable security arrangements are implemented across the university.

22.00 The Vice-President Finance and Operations may approve the implementation of temporary actions as listed in section 28.00 of this policy.

23.00 In relation to paper-based Information Resources, the General Counsel and the University Secretary in conjunction with the University Archivist:

- create awareness across the University Community about members' responsibilities within this policy; and
- establish processes for compliance with reasonable security arrangements through the Records Management and Protection of Privacy policies and procedures.

24.00 Administrative Authorities within their role outlined in 19.00 above must:

- identify the electronic Information Resources for which they are responsible and communicate those to the Chief Information Officer;
- define the purpose and function of Information Resources and ensure that requisite education and documentation are provided to the university;
- establish acceptable levels of security risk for Information Resources by assessing factors such as the:
    - sensitivity of the Information Resource;
    - criticality of the Information Resource to the continuing operation of the area in their control, including related research projects or other essential associated activities;
    - impact of security issues created in the area under their control that may affect other areas or the university as a whole;
    - likelihood that an Information Resource could be used as a platform for inappropriate acts;
    - limits of available technologies, programmatic needs, cost, and staff support; and
- ensure that reasonable security arrangements are implemented for the Information Resources for which they are responsible.

25.00 Providers must:

- be knowledgeable of relevant security policy, procedures, standards, and guidelines;
- analyze potential threats and the feasibility of various security arrangements in order to provide recommendations to Administrative Authorities;
- implement security arrangements that may mitigate threats, consistent with the level of risk established by Administrative Authorities;
- establish procedures to ensure that privileged accounts are kept to a minimum and that users comply with privileged access agreements; and
- communicate the purpose and appropriate use for the Information Resources for which they are responsible.

26.00 Users must:

- make a reasonable effort to become familiar and comply with this policy and its associated procedures, standards, and guidelines;
- protect the Information Resources for which they are responsible in accordance with this policy and its associated procedures; and
- consult, as necessary, with the appropriate authority regarding this policy and its associated procedures.

27.00 This policy must be implemented when receiving or sharing Information Resources with other Units, legal entities, or persons, including but not limited to educational, governmental, charitable, and private sector organizations.

<u>Compliance</u>

28.00 The Information Security Office will investigate suspected violations of this policy; recommend or implement corrective action; suspend, disable, terminate, or remove

access to or from Information Resources; or take other action in accordance with collective agreements and university policies and procedures.

29.00 Where suspected violations of this policy involve personal information, the General Counsel, where appropriate in consultation with the Information Security Office and/or Campus Security, will initiate an investigation and may recommend appropriate action.

30.00 Where there is a suspected breach of physical security of paper records not involving personal information, Campus Security will investigate and may recommend appropriate action.

**AUTHORITIES AND OFFICERS**

31.00 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*

**RELATED POLICIES AND DOCUMENTS**

Associated Procedures:

- Procedures for Responding to an Information Security Incident
- Procedures for Addressing Security Vulnerabilities of University Information Resources and Information Systems
- University Information Security Classification Procedures
- Procedures for Responding to the Loss or Theft of a Mobile Computing Device
- Payment Card Acceptance Procedures
- Guidelines for the Secure Destruction and Deletion of University Records and Information

Protection of Privacy Policy (GV0235) and associated procedures

Records Management Policy (IM7700) and associated procedures

Acceptable Use of Electronic Information Resources Policy (IM7200)

Key and Access Card Control Policy (BP3125)

Directory of Records

Enterprise Data Access Protocol

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
**Parent Policy:** Information Security Policy (IM7800)

**Effective Date:** Dec, 2010
**Supersedes:** New
**Last Editorial Change:** July 2018

## 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.

## PROCEDURES

*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.*

Identification and Reporting

3.00 Any member of the University Community, as well as external third parties, may report Information Security Incidents.

3.01 Information Security Incidents must be reported to the university's Information Security Office.

4.00 The Information Security Office will create an Information Security Incident report and 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.

The Incident's severity will be determined based on factors such as the:

- sensitivity and criticality of the information or information systems;
- operational impact on the university or a Unit;
- magnitude of the service disruption;
- threat potential;
- expanse or scope of the Incident;
- impact to the University's reputation; or
- other adverse impacts on the university, individuals, or third-parties.

5.00 Where it appears to the Information Security Officer that there has been a significant Information Security Incident, the Information Security Officer will inform the Chief Information Officer.

5.01 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.

5.02 Where the Information Security Incident does or may involve the unauthorized disclosure of Personal Information, the Information Security Office will inform the Privacy and Access Office.

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

- the Information Security Officer
- the Chief Information Officer
- the Administrative Authority responsible for the information or Information Systems involved.

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

- University Secretary
- Chief Privacy Officer
- Associate Vice-President Human Resources
- General Counsel
- Associate Vice-President Faculty Relations and Academic Administration
- Executive Director, University Communications + Marketing
- Director, Campus Security
- Manager, Computer Help Desk
- other Administrative Authorities
- other subject matter experts

<u>Containment</u>

7.00 The Chief Information Officer (or designate), in collaboration with the Administrative Authority or Provider responsible for the Information Resource, will take steps to ensure the requisite Unit(s) makes reasonable efforts to contain the Incident by, for example:

- stopping the unauthorized practice;
- recovering the information or records that were improperly collected, used, disclosed, or disposed of;
- shutting down affected systems;
- revoking access;
- changing computer access codes;
- blocking network access; or
- correcting weaknesses in physical security.

Where a unit is not able to take the steps recommended, a request will be submitted to the Vice-President Finance and Operations to approve further investigation.

7.01 In instances where the Chief Information Officer (or designate) assesses that the incident is significant, and time is of the essence, the Chief Information 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 Vice-President Finance and Operations will be required before taking this step.

Eradication

8.00 After an Information Security Incident has been contained, the Administrative Authority or Provider responsible for the Information or Information Systems involved, in collaboration with the Information Security Office, will take action to eliminate the problem or mitigate vulnerabilities that may allow a reoccurrence of the Incident.

Recovery

9.00 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:

- restoring information or Information Systems from backups;
- validating that the information is complete and accurate or that an Information System is operating correctly; or
- performing additional monitoring.

Follow-up and Correction

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

11.00 Once all investigations are complete, the response team will provide a report of the Incident to the appropriate Administrative Authorities which may include:

- a summary of the incident;
- corrective actions taken;
- recommendations made for additional safeguards;
- follow-up actions required; and
- lessons learned.

## RELATED POLICIES AND DOCUMENTS

Protection of Privacy Policy (GV0235)

- Procedures for Responding to a Privacy Incident or Breach
- Procedures for the Management of University Surveillance Systems
- Procedures for the Disclosure of Student Personal Information in Emergency or Compelling Circumstances
- Procedures for the Management of Personal Information
- University Information Security Classification Procedures

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

Records Management Policy (IM7700)
- Procedures for Access to and Correction of Information
- Procedures for the Management of University Records
- Guidelines for the Secure Destruction and Deletion of University Records and Information

Information Security Policy (IM7800)
- Procedures for Responding to an Information Security Incident
- Procedures for Responding to the Loss or Theft of a Mobile Computing Device
- Payment Card Acceptance Procedures
- University Information Security Classification Procedures
- Procedures for Addressing Security Vulnerabilities of University Information Resources and Information Systems

University of Victoria

# PROCEDURES FOR ADDRESSING SECURITY VULNERABILITIES OF ELECTRONIC UNIVERSITY INFORMATION RESOURCES AND INFORMATION SYSTEMS

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

**Effective Date:** Jun, 2017
**Supersedes:** Dec, 2010
**Last Editorial Change:** July 2018

## 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 Resources or Information Systems' security.

## DEFINITIONS

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

3.00 **Vulnerability** means an identified security weakness in a university Information Resource or Information System that could lead to a Security Incident.

## PROCEDURES

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 Resources 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 either be:

(a) recognized by the Information Security Office as part of regular network and Information System monitoring, assessment, or maintenance; or

(b) reported to the Information Security Office when a Provider, Administrative Authority (or designate), or other individual becomes aware of a Vulnerability.

Preliminary Assessment

5.00 Where the Information Security Office becomes aware of a Vulnerability in an Information Resource or Information System, the Information Security Office will conduct an initial assessment in order 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:

- sensitivity and criticality of the Information Resource or Information Systems involved;
- likelihood of the Vulnerability causing a Security Incident;
- operational impact to the university or a Unit;
- operational impact on other Information Resources or Information Systems;
- threat potential; and
- 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 a university Information Resource or 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 and/or Provider of the requisite Unit(s) and to the Chief Information Officer.

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

6.02 In instances where the Chief Information Officer (or designate) assesses that the Vulnerability is significant, and time is of the essence, the Chief Information 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 in the affected Unit(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 Vice-President Finance and Operations will be required before taking this step.

7.00 Where the Chief Information 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 Officer (or designate) after working with the Administrative Authority may seek approval from the Vice-President Finance and Operations to 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 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 requisite Unit(s).

**RELATED POLICIES AND DOCUMENTS**

Information Security Policy (IM7800)

- Procedures for Responding to an Information Security Incident
- Procedures for Responding to the Loss or Theft of a Mobile Computing Device

Protection of Privacy Policy (GV0235)

- Procedures for Responding to a Privacy Incident or Breach

Records Management Policy (IM7700)

- Procedures for the Management of University Records
- Guidelines for the Secure Destruction and Deletion of University Records and Information

University of Victoria

# UNIVERSITY INFORMATION SECURITY CLASSIFICATION PROCEDURES

**Procedural Authority:** Vice-President Finance and Operations
**Procedural Officer:** Chief Information Officer

**Effective Date:** January, 2015
**Supersedes:** December, 2010
**Last Editorial Change:**

**Parent Policies:** Information Security Policy (IM7800)
Protection of Privacy Policy (GV0235)

---

## 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 require security classification 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 and procedures. Units may also refer to industry standards and best practices for further direction where applicable.

4.00 Administrative Authorities are expected to 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 are expected to ensure 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. 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 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. 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. | Minor 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.<br>• Principles of least-privilege and need-to-know must be applied<br>• 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.<br>• Principles of least-privilege and need-to-know must be applied<br>• 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.<br>• Access must be revoked as soon as reasonably possible when Users leave the university or the custodial Unit. | • No access restrictions |
| **Transmission** | • Encryption for public networks (e.g. wireless, Internet).<br>• Encryption strongly-recommended on trusted, internal networks.<br>• Third-party email providers are not appropriate for transmitting.<br>• Data may be masked instead of encrypting.<br>• Double envelope mailings for hardcopy records | • Encryption for public networks (e.g. wireless, Internet).<br>• Encryption strongly recommended on trusted, internal networks.<br>• Third-party email providers are not appropriate for transmitting.<br>• Data may be masked instead of encrypting.<br>• Clearly marked “confidential” on sealed mailings. | • Encryption strongly recommended on public networks (e.g. wireless, Internet) | • 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.<br>• Encryption mandatory on mobile devices and workstations, and | • Stored within a controlled-access system (e.g., password protected file or file system, locked file cabinet, alarmed area).<br>• Encryption mandatory on mobile devices and workstations, and strongly-recommended in all environments<br>• Implement “clean desk” policy<br>• Must be stored in Canada | • Stored within a controlled-access system (e.g., password protected file or file system, locked file cabinet).<br>• Encryption strongly recommended in all environments. | • No special safeguards required. |

| | | | | |
|---|---|---|---|---|
| | strongly recommended in all environments.<br>• Implement “clean desk” policy<br>• Must be stored in Canada | | | |
| **Destruction** | • Shredded or 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 | • 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

**RELATED POLICIES AND DOCUMENTS**

Information Security Policy (IM7800)

Procedures for Responding to an Information Security Incident

Protection of Privacy Policy (GV0235)

Procedures for Responding to a Privacy Incident or Privacy Breach

Procedures for the Management of Personal Information

Procedures for the Management of University Surveillance Systems

Records Management Policy (IM7700)

Procedures for the Access to and Correction of Information

Procedures for the Management of University Records

Guidelines for the Secure Destruction and Deletion of University Records and Information

Responsible Use of Information Technology Resources (IM7200)

## APPENDIX A: INFORMATION CLASSIFICATION EXAMPLES

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

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

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

| | |
|---|---|
| **Prohibited** | *Credit Card Data / Payment Card Industry Data Security Standard (PCI DSS) (when taken as part of a financial transaction)*<br>• Service Code<br>• ISO Number<br>• CVC2, CVV2 or CID value<br>• PIN or PIN block<br>• 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 MOBILE COMPUTING DEVICE

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

**Effective Date:** December, 2010
**Supersedes:** New
**Last Editorial Change:** July 2018

---

## 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 Mobile Computing Device in order to protect the information contained on the device.

## DEFINITIONS

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

3.00 **Mobile Computing Device** means any portable device that provides computing or information storage and retrieval including but not limited to: laptop computers, Personal Digital Assistants (PDA), cell phones, smart phones, flash drives, video cameras, compact disks (CD), digital video disks (DVD), and portable hard drives.

## PROCEDURES

User Responsibility

4.00 Users of university Mobile 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

5.00 Loss or theft of a university Mobile Computing Device must be immediately reported to Campus Security and to the Unit's Administrative Authority.

5.01 When reporting the loss or theft, Users are expected to inform Campus Security of whether the Mobile Computing Device contains Personal Information, or information classified as Internal, Confidential or Highly Confidential under the university's Information Classification procedure.

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

7.00 Campus Security shall immediately inform the Information Security Office if the lost or stolen Mobile Computing Device contains:
(a) Personal Information; or
(b) Internal, Confidential, or Highly-Confidential information (as defined in the University Information Security Classification procedures).

8.00 Where the Information Security Office confirms that the lost or stolen Mobile Computing Device contains Personal Information, the Information Security Office shall immediately contact the General Counsel.

Response

9.00 In cases where Personal Information is contained on a lost or stolen Mobile Computing Device, the General Counsel, where warranted, will follow the Procedures for Responding to a Privacy Incident or Privacy Breach.

9.01 Where the information contained on the Mobile 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**

Protection of Privacy Policy (GV0235)
- Procedures for Responding to a Privacy Incident or Privacy Breach

Records Management Policy (IM7700)
- Procedures for Access to and Correction of Information
- Procedures for the Management of University Records
- Guidelines for the Secure Destruction and Deletion of University Records and Information

Information Security Policy (IM7800)
- University Information Security Classification Procedures
- Procedures for Responding to an Information Security Incident

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:** June, 2012
**Supersedes:** New
**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.

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

The purpose of this procedure is to establish responsibilities and expectations of university Units who accept Payment Cards.

## DEFINITIONS

2.00 **Cardholder** means an individual with a Payment Card.

3.00 **Financial Services** refers to the Department of Financial Services

4.00 **Merchant** refers to 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.

5.00 **Payment Cards** refer to credit cards, debit cards, and other media that are presented by individuals for the purpose of making payments.

6.00 **Payment Processor** refers to the third party service provider that Financial Services has engaged to process Payment Card transactions on behalf of university Merchants.

7.00 **Payment Card Industry-Data Security Standards (PCI-DSS)** 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.

8.00 **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**

9.00 These procedures apply to all Units which process university Payment Card transactions in any form and which may include:

- websites (eCommerce),
- PIN entry devices (PEDs),
- departmental information systems
- manual entry by staff from information provided by Cardholders (fax, telephone, forms.

**PROCEDURES**

10.00 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.

11.00 All applications for Merchant accounts are to be submitted to Financial Services.

12.00 Units looking to implement new systems or replace existing systems must consult with Financial Services (Manager, Treasury Services) and University Systems prior to proceeding in order to ensure systems are PCI-DSS compliant.

13.00 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.

14.00 Units must implement mechanisms to ensure that 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.

15.00 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.

16.00 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.

17.00 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.

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

19.00 Units are responsible for retaining appropriate transaction records for audit purposes for a period of seven years.

20.00 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.

21.00 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 Resources and Information Systems.

22.00 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.

**RELEVANT LEGISLATION**

*Freedom of Information and Protection of Privacy Act*
*Personal Information Protection Act*

**RELATED POLICIES AND DOCUMENTS**

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
Signing Authority Policy (FM5100)
Information Security Policy (IM7800)
Protection of Privacy Policy (GV0235)

University of Victoria

# GUIDELINES FOR THE SECURE DESTRUCTION AND DELETION OF UNIVERSITY RECORDS AND INFORMATION

**Procedural Authority:** University Secretary, Vice-President Finance & Operations
**Procedural Officers:** University Archivist and Chief Information Officer

**Effective Date:** November, 2014
**Supersedes:** July 2014
**Last Editorial Change:**

**Parent Policies:** Records Management Policy (IM7700)
Information Security Policy (IM7800)

---

## PURPOSE

1.00 The purpose of these guidelines is to protect Records and information in the custody or under the control of the university from unauthorized use or disclosure by informing university employees of:

1.01 How to conduct the physical destruction of paper Records and electronic devices containing information that is classified as Internal, Confidential or Highly-Confidential under the university Information Security Classification procedures, or designated in the Directory of Records as requiring confidential destruction; and

1.02 How to conduct deletion of information in electronic form that is classified as Internal, Confidential or Highly-Confidential under the university Information Security Classification procedures, or designated in the Directory of Records as requiring confidential destruction.

## DEFINITIONS

2.00 The definitions contained within the university's Records Management (IM7700) and Information Security (IM7800) policies apply to these procedures.

3.00 **Secure Destruction** means permanent physical destruction of paper records and electronic devices, rendering unreadable or unrecoverable the information they contain.

4.00 **Deletion** means removal of information from electronic devices and storage media.

4.01 **Routine Deletion** means removal or erasure of information from electronic devices and storage media by marking information as deleted. The information still exists, making data recovery possible unless the information is securely deleted or overwritten.

4.02 **Secure Deletion** means the process of deliberately, permanently, and irreversibly removing or erasing information from electronic devices and storage media.

5.00 Sanitization is a process to render access to target data (the data subject to the sanitization technique) on the device or media either effectively inaccessible (but potentially recoverable through data recovery techniques) or effectively irrecoverable. Deletion, erasure (deletion with overwriting), and destruction (physical destruction of the storage media) are actions that can be taken to sanitize media.

**SCOPE**

6.00 These guidelines apply to the following actions taken after the decision to dispose of Records and information consistent with Directory of Records (DOR) retention rules has been made:

6.01 The physical destruction of information, whether in paper, electronic, audio-visual or other format. This includes computers and other electronic devices and storage media (e.g. mobile phones); see section 16 below for further examples; and

6.02 The deletion of information in electronic form.

**GUIDELINES**

7.00 The method for Secure Destruction must be appropriate for the medium on which the information is stored.

Security Classification

8.00 Units are expected to refer to the security classification level of the information and Records prior to their destruction to assist in determining an appropriate destruction method. (See http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf)

Authorization for Secure Destruction and Secure Deletion

9.00 Unit offices identified as Primary Offices for a particular Record series are responsible for obtaining authorization for Disposition from the University Archives prior to Secure Destruction or Secure Deletion in accordance with the university's Procedures for the Management of University Records (http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf and the Directory of Records. See

http://www.uvic.ca/library/locations/archives/records_management/resources.php for authorization forms.

9.01 Unit offices identified as Secondary Offices for a particular Record series may securely destroy or delete Records past their retention period without authorization from the University Archives.

Units are encouraged to consult the University Archives for specific guidance on Records Disposition, including Secure Destruction or Secure Deletion if they are not already familiar with the Disposition process.

Primary Office is an office or offices responsible for keeping the original and/or official versions of Records. Secondary Office is an office or offices which may hold duplicate copies of university Records that are to be maintained for shorter retention periods than original and/or official versions of Records.

Secure Destruction of Paper-Based Information

10.00 Records containing Highly-confidential, Confidential, and Internal information are to be shredded in a secure manner; Records containing public information may be recycled.

10.01 Records containing Highly-confidential information (see Information Security Procedures) should be shredded by a staff member of the Unit that holds the records, or on campus ("onsite") by an external supplier. Records containing Confidential or Internal information may be shredded off campus ("offsite") by an external supplier, or onsite by an external supplier or by a staff member of the Unit that holds the records.

| Information Security Level | Highly-Confidential | Confidential | Internal | Public |
|---|---|---|---|---|
| **Destruction, Paper Records** | Onsite shredding | Offsite shredding (Onsite optional) | Offsite shredding (Onsite optional) | Recycle |

11.00 Units should use the university's preferred external suppliers for shredding services. For supplier names, information on engaging them, and negotiated pricing, see http://www.uvic.ca/purchasing/faculty-staff/preferred-suppliers/index.php (requires NetLink logon).

11.01 If a Unit does not wish to use the preferred external suppliers for shredding services, the following conditions must be met:
- The external supplier must be NAID certified
- The service is selected in accordance with the Purchasing Services Policy (FM5105).

12.00 Units may consider the appropriateness of a Unit staff member supervising shredding by an external supplier, but this is not required.

13.00 Small quantities of paper Records may be shredded by individual Units. Contact Purchasing Services for recommended shredder models if necessary.

- If a Unit uses its own shredders, the Records must be shredded in a secure manner; secure methods include shredding into strips that are a maximum of one centimetre wide, cross-cut shredding, re-shredding or mixing shredded Records to ensure that information cannot be reconstructed.
- For Records with Confidential or Highly-confidential information, cross-cut shredding or re-shredding is recommended.
- If such Records are not cross-cut shredded or re-shredded, the shredded Records should be mixed to ensure information cannot be reconstituted.

If a staff member of a Unit is uncertain about the security classification of the information or Record, the staff member shall use the destruction method for the higher level. Contact the Records Management Archivist with questions.

13.00 Records awaiting Secure Destruction must be kept in a secure manner (i.e. locked cabinet, controlled access area, secure supplier's console, or sealed boxes in a locked room).

Electronic Device or Storage Media Sanitization

15.00 The approach for handling electronic devices and storage media after use is dependent on whether the devices or media are being repurposed for university use or are no longer required for use.

Deletion of Electronic Device or Storage Media Information

16.00 Electronic devices and storage media purchased with university funds or funds administered through the university, and that are repurposed for university use, must have information Sanitized prior to being repurposed.

16.01 Electronic devices and storage media that will be repurposed for university use that contain information classified as Public or Internal may be Sanitized by Routinely Deleting all data on the device in a manner that renders it effectively inaccessible.

16.02 Electronic devices and storage media that will be repurposed for university use that contain information classified as Confidential or Highly-confidential must be Sanitized using a method that erases data by overwriting the data multiple times, prior to being repurposed to another Unit or employee. Erasing overwrites all addressable locations with a character, its complement, then a random character, and verifies. If you require assistance, contact the Computer Help Desk to arrange for erasing of devices and storage media. http://www.uvic.ca/systems/services/contact/index.php

16.03 For best practices on Deletion and erasure, please see the "How To" section on the following University Systems service page: http://www.uvic.ca/systems/services/informationsecurity/diskencryption/index.php

Destruction of Electronic Devices or Storage Media

17.00 Electronic devices and storage media purchased with university funds or funds administered through the university, that are not repurposed for university use, must undergo secure physical destruction when no longer required by a Unit or employee, whether or not they are known to store Internal, Confidential, or Highly-confidential information.

17.01 Units must use the central secure physical destruction program provided by University Systems and Purchasing Services. Contact the Computer Help Desk to arrange for Secure Destruction of electronic devices and storage media. http://www.uvic.ca/systems/services/contact/index.php

17.02 Electronic devices and media requiring secure physical destruction include, but are not limited to: hard drives, flash media, USB keys, thumb drives, CDs, DVDs, floppy disks, computer tapes, audio and video storage devices, PDAs, Smart Phones and cell phones, and hard drives in all printers and copiers.

**RELATED POLICIES AND DOCUMENTS**

Protection of Privacy Policy (GV0235)
- Procedures for Responding to Privacy Incidents or Privacy Breach

Records Management Policy (IM7700)
- Procedures for Access to and Correction of Information
- Procedures for the Management of University Records

Information Security Policy (IM7800)
- University Information Security Classification Procedures
- Procedures for Responding to an Information Security Breach

**RESPONSIBLE OFFICES**

Information Security Office
University Archives