

Information Security Incident Reporting Policy

Effective Date: March 01, 2012

Review Date: March 01, 2017

Approving Body: Mike Langedock, Chief Information Officer

Applies to: All Faculty, Staff and Students and Sponsored Users

1.0 Reason for Policy

Establishes the requirement to report information security incidents to appropriate University officials. Reporting of information security incidents is necessary to ensure that proper and timely response procedures can be initiated to control, eliminate, investigate and document events that could potentially disrupt the operation of the university or compromise university records.

Reporting also enhances awareness of trends in security incidents that indicate the need for adjustments in the University's security program.

All affected users of this policy are expected to report information security incidents as soon as possible.

2.0 Policy Statement

2.1 What is a reportable information security incident?

An information security incident is any real or suspected adverse event, regardless of accidental or malicious cause, that could lead to a breach of IT policy, security, confidentiality or legislation. In summary these can be described as:

- the act of violating an explicit or implied IT security policy,
- access or disclosure, either intended or unintended, of University records to any unauthorized individuals,
- the unauthorised alteration of University records,
- unwanted disruption or denial of service,
- the unauthorised use of a system for the processing or storage of data,
- the loss of data for which the University is legally or contractually bound to protect,
- unexpected changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent

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

- unauthorised use of an individual's computer account,
- attempts (failed or successful) to gain unauthorised access to a system or its data
- loss, theft or damage of electronic devices, electronic media, or paper records that contain sensitive University records including records subject to *The Freedom of Information and Protection of Privacy Act* (FIPAA) and *The Personal Health Information Act* (PHIA),

- malicious software installations on systems or devices that store sensitive University records including those subject to the FIPPA and PHIA Policy,
- defacement of a University website,
- use of computing resources for unethical or unlawful purposes,
- contact by any law enforcement or intelligence organisation regarding a University owned electronic device that may be used to commit a crime.

Routine detection and remediation of a “virus”, “malware” or similar issue that has little impact on the day-to-day business of the University, is not considered an incident under this policy.

2.2 Adverse impacts of an Information Security Incident

An information security incident may have a range of adverse impacts including, but not limited to:

- disruption of activities,
- threat to personal safety or privacy,
- reputational damage to the University and/or its students, staff and faculty
- legal obligation or penalty,
- financial loss.

2.3 Incidents Requiring Special Reporting Procedures

Under provincial legislation, the University of Manitoba is subject to FIPPA and PHIA. To comply with these legislative requirements, the University must follow detailed procedures when reporting a breach of security involving personal information and personal health information.

Under the legislation, a breach of security occurs whenever personal or personal health information records (electronic or non-electronic) are improperly collected, used, disclosed, destroyed other than as authorized, or when the integrity of the information is compromised. The University’s “FIPPA and PHIA Policy and Procedures” provide complete details on the reporting procedures of such incidents.

Examples of such incidents that are subject to these special reporting procedures include, but are not limited to:

- an email, fax, or paper document containing Personal Information or Personal Health Information sent to unintended recipients,
- unauthorised disclosure of personal information or personal health information,
- loss of electronic storage media or mobile storage device containing personal information or personal health information
- finding paper or electronic records about identifiable individuals in any location outside of the authoritative premises,
- personal information or personal health information lost in transit
- the inability to demonstrate with authority the integrity of a system containing personal or personal health information

2.4 Suspected Incidents

Often very little information is obtained in relation to an incident and it may be uncertain whether an actual incident has taken place. Suspected incidents should always be reported as they often provide information that can be used to mitigate the risk and impact of future events.

2.5 Initial Reporting of Information Security Incidents

All information security incidents should be reported, in the first instance to:

IST Help and Solutions Centre
Fort Garry (Mon-Fri 8:00am to 8:00pm)
204-474-8600
123 Fletcher Argue
support@umanitoba.ca

Bannatyne (Mon-Fri 8:30am to 4:30pm)
204-789-3541
231A Neil John Maclean Library
help_desk@umanitoba.ca

2.6 Other Reporting Options

In certain circumstances, due to the sensitive nature of an incident, reporting may be done directly to the:

IT Security Coordinator
204-474-8340
itsecure@cc.umanitoba.ca

or

Access and Privacy Officer
204-474-8339

3.0 Accountability

3.1 The Chief Information Officer is responsible for the communication, administration and interpretation of this Policy.

3.2 Deans, Director's and Department Heads should ensure these practices are communicated to faculty, staff and students and are adhered to.

4.0 Cross References

Acceptable Use of Computer Resources
Use of Computer Facilities
FIPPA and PHIA
Mobile Device Policy