Standard: Information Security Incident Handling

Effective Date:	2016.11.30
Revision Date:	2022.02.06
Review Date:	2024.01.31
Approving Body:	Director, Information Security and Compliance
Authority:	Information Security Policy
Responsible Owner:	Director, Information Security and Compliance
Classification:	Public

Purpose

The Information Security Incident Handling Standard establishes the requirement to report information security incidents to appropriate University officials and describes the incident handling process. 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.

Who/what does the standard apply?

The requirements in this standard apply to all:

- Students
- Academic staff
- Support staff
- IT Support
- Contractors
- Sponsored Users
- Vendors

Definitions

- **Information Security Incident:** 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.
- **IT Support:** All staff in a unit or faculty who are responsible for maintaining computer systems and hardware, and for making decisions pertaining to those systems.

Compliance

All information security incidents should be reported to the Information Security and Compliance team through one of the following options:
infosec@umanitoba.ca, abuse@umanitoba.ca, spam@umanitoba.ca, servicedesk@umanitoba.ca

Specifications

What is a reportable information security incident?

An information security incident is any real or suspected event that may adversely affect the security of the University's information or the systems that process, store, or transmit that information. Examples may include, but are not limited to:

- 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 University records
- malicious software installations on systems or devices that store University records
- defacement of a University website,
- use of computing resources for unethical or unlawful purposes.

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.

Information Security Handling Process

Process Description

Security incidents will be prioritized according to the severity of the incident in order to determine the appropriate response. The following factors are considered in determining the priority of an incident:

- Scope of impact
- Criticality of the system or service
- Sensitivity of the information
- Probability of propagation

Four levels of incident priority will be used to guide incident response: HIGH, MEDIUM, LOW

The following steps will be used to identify, prioritize, manage and resolve security incidents.

Triage

Once a potential security incident is reported or anomalous activity detected, analysis must be performed to determine if it is indeed symptomatic of a security incident and to understand the nature of the incident for proper remediation.

The security incident detected or reported will be prioritized, leading to the assignment of a Level for the incident which will drive the remaining incident management process. An incident response team will also be identified during this step, and an entry will be added to the Information Security

Investigate

During the investigation an understanding of the nature and scope of the incident is refined, and validation of the Level will take place. If confidential data is involved that must be noted, as it will impact the documentation that will be collected.

Incident Classification and Type

Incidents may be classified as one of the following:

Abusive Content, Malicious Code, Information Gathering, Intrusion Attempts, Intrusion, Availability, Information Content Security, Fraud, Vulnerable Other

The incident type may be one or more of the following:

Spam, Harmful Speech, Violence/Racism, Malware, Scanning, Sniffing, Social Engineering, Exploiting known Vulnerabilities, Brute Force Attack (Login Attempts), Account Compromise, Application Compromise, DoS (Denial of Service), Sabotage, Outage (No Malice), Unauthorized Access to Information, Unauthorized Modification of Information, Unauthorized Use of Resources, Copyright, Masquerade or False Representation, Phishing, Open for Abuse, False Positive, Breach of Policy of Standard, Other

Containment

Once a security incident in confirmed, classified, and categorized, the next step is typically containment. It is important to stop the potential loss of confidential data, protect other computers and information on the campus network and Internet (for example, keep the malware from spreading to other computers on or off campus), prevent further damage to the compromised system and/or information, and identify the location and owner of the computer(s) so they can be engaged in containment and remediation.

Containment activities are designed to prevent further damage and are specific to the security incident. A long term risk mitigation solution may not be known at this time.

Eradication and Recovery

Eradication and recovery activities may include preserving evidence if required and it has not already been done; performing additional analysis as needed to complete the investigation, removing the components of the incident impacting the affected systems (such as deleting the malicious code or disabling a compromised user account), taking steps so a similar incident does not occur (for example, patch the vulnerability used to compromise the system, apply standard system hardening procedures, adjust firewall rulesets, etc.) and restoring systems to normal operation.

Communication

Incident Communication is invoked from many aspects of the end-to-end Incident Response. The communication process ensures that information is captured and communicated effectively during triage, handling, and response qualification.

Notification of an incident is a final outcome of the triage process. Proper and timely notification of incidents to appropriate owners with accurate, relevant information is critical to the process. Reporting lessons learned including details of the incident, decisions made, outcomes and outstanding decisions or activities is part of incident communication activities.

Close and Lessons Learned

The close activities will include documenting lessons learned and making recommendations to prevent subsequent similar incidents, issuing final reports, archiving any evidence and documentation, and closing the incident. A Post-Mortem Review session may be required.

References

Policy, Procedure or Standard	
Information Security Policy and Procedure	
Incident Handling Process Documentation (Detailed Process Guide)	