UNIVERSITY OF TORONTO	**Document Status:** **Approved**	**Document type**	**Standard**
		Revision #	1.0
		Endorsement and Approval Date	March 3, 2021
Name	**INCIDENT RESPONSE PLAN**	**Last Reviewed/Update Date**	February 24, 2021
Approved by			

Table of Contents

1.0 Introduction

Information Security Incident response is a vital component of adequate information and cyber risk management. Effective incident response is a complex and multi-dimensional undertaking whose success depends on planning and resources. The Incident Response Plan provides guidance for managing incident response with the primary objective to contain and mitigate the risks and issues associated with computer security incidents.

This document also outlines the high-level process and requirements for responding to and resolving security incidents such as:

- Phishing attacks,
- Malware and viruses,
- Denial of resources or services,
- Unauthorized access or attempts to gain unauthorized access,
- Inappropriate use of network resources,
- Data breaches,
- Changes to system hardware, firmware or software without owner's knowledge
- Any other unlawful activity involving computer networks and processing equipment.

The use of this plan will provide respondents dealing with an incident with the following:

- A basic overview of the most common types of incidents.
- Direction for classifying the severity of an incident.
- Based on the severity, direction for who should and who must be notified.
- Recommendations for the makeup and responsibilities of the incident response team.
- Relationships to other policies and procedures and playbooks.

Incident Response Plan is an essential element of the Risk Management Program. All units shall have an Incident Response Plan in place that is reviewed annually and ensure appropriate training and operational readiness to respond to an information security incident.

This plan addresses only adverse events that are information security-related, not those caused by natural disasters, power failures, etc.

1.1 Purpose

The purpose of this document is to:

1. Outline a process for responding to information security incidents along with roles and responsibilities.
2. Define the classification of information security incidents.
3. Provide a resource toolkit on Incident Management Training (proactive) and Handling (during a live incident).

1.2 Audience

The primary audience for this plan includes all IT managers, non-IT unit leaders and all other employees at the University of Toronto who need to be aware of the incident response process and be able to escalate incidents to their leadership teams, including divisions/departments/faculties responsible for conducting or involved with information security investigations.

Additionally, all IT professionals at the University shall review the document to become familiar with the Incident Response process.

1.3 Maintenance

The Incident Response Workgroup under the Information Security Council will review and maintain this document on an annual basis. As such, this document's audience shall review this document in the same frequency after its publication.

1.4 Authority

The Chief Information Security Officer (CISO) or their delegates are charged with executing this plan by virtue of its original charter and the Policy on Information Security and the Protection of Digital Assets.

1.5 Relationship to other Policies

This plan supports the implementation of the Policy on Information Security and the Protection of Digital Assets.

1.6 Relationship to Other Groups at the University

The Information Security (IS) department acts on behalf of the University community to manage security incidents and will ask for cooperation and assistance from community members as required. The IS also works closely with University administrative groups such as the Student Life Office, Human Resources, and the Office of General Counsel and FIPP in investigations and e-discovery matters. At their behest or if directly requested, IS may also assist Law Enforcement.

2.0 Definitions

2.1 Event

An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending an email, and a firewall blocking a connection attempt.

2.2 Adverse event (Alerts)

Adverse events (alerts) are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and the execution of malware that destroys data.

Machine or human analysis triggers Alerts, and those alerts can lead to security incidents.

2.3 Security Incident

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data about the organization and threatens to release the details publicly if it does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file-sharing services.

In the University of Toronto context, incidents may be violations of the Policy on Information Security and the Protection of Digital Assets, Policy on the Acceptable Use of Information and Communication Technology, other University policy, security standards, or code of conduct, or threatens the confidentiality, integrity, or availability (CIA) of Information Systems or Institutional Data.

Incidents are established from many vectors, including but not limited to:

- Monitoring systems,
- Reports from faculty, staff and students,
- Outside organizations,
- Service degradations or outages.

Discovered incidents shall be declared and appropriately documented. IT security-related incidents may also cause service outages.

2.4 Data

Data in the context of an incident is the data that has been or could have been accessed, exfiltrated, or publicly exposed due to the incident. The data could reside on a compromised device or in another directly connected device or another device in the same network environment.

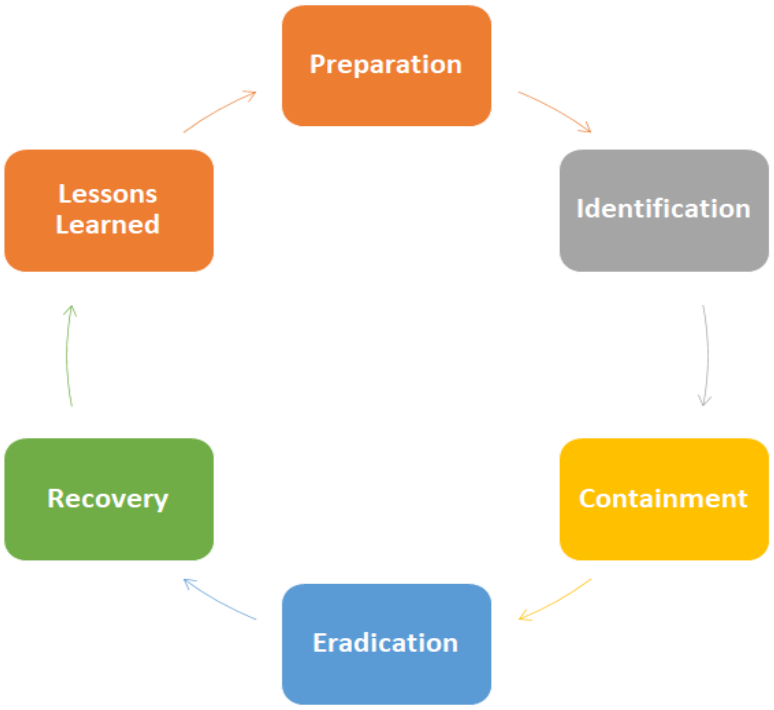
The University of Toronto Data Classification Standard identifies four data levels and what data types are included in each level.

Depending on the type of data exposed, the University may be responsible for different notification levels to the government or private bodies. These are the three primary Laws' or agreements related to data that the University may need to report to are:

- **Personal Health Information Protection Act (PHIPA)**
  PHIPA is specific to health information and, in this context, the security of that data.
- **Freedom of Information and Protection of Privacy Act (FIPPA)**
  FIPPA is related to personal data, and many things can fall under its purview, including communications with students, UTORids, Employee records and research data. IS and the FIPP office can help clarify what does or doesn't fall under FIPPA as data is identified.
- **Payment Card Industry Data Security Standard (PCI DSS or PCI)**
  PCI is explicitly associated with credit card information and disclosure. In particular, exposure of full credit card numbers and expiry dates or magnetic stripe data is of concern.

3.0 Overview of the Incident Response Process

Planning and preparing for an information security incident can be challenging for many units inside the University. When an information security incident occurs, a Unit is required to take immediate action to mitigate threats to the Confidentiality, Integrity, and Availability of its information assets. The effort requires the effective deployment of resources and established communication strategies. The Incident Response team will typically follow six high-level steps:



- **Preparation** — Includes documentation, testing, training and other preparatory activities.
- **Identification** — Includes the confirmation that an incident has occurred and the initial severity level. It identifies what data, devices, or systems were damaged, accessed, or exposed as part of the breach. Additionally, it includes the collection of logs, system images, and other artifacts. Activation of the CSIRT happens at this time if required.
- **Containment** — Initial short-term containment of the incident will typically entail the disconnection of affected services, devices or networks to limit additional damage or malicious activity.
- **Eradication**— Identify the root cause of the incident. Remove malware, malicious code and vulnerabilities from all affected systems using the identification step's collected information.
- **Recovery** — Return systems carefully back to production status, ensuring mitigation of the root cause occurs first.
- **Lessons learned** — Review the root cause of the incident and identify opportunities to improve detection and defences to lessen a reoccurrence chance. Also, review the process of dealing with the incident and determine any improvements there as well.

4.0 Severity Ratings of Incidents

Categorization of Incidents is based on the potential for exposure of sensitive data or the resource's criticality using a High-Medium-Low designation. The severity rating initially applied can be adjusted during the plan's execution as identification of the scope and contents of the systems involved progresses.

4.1 Security Incidents – Severity Categories

High:

Significant fines, penalties, regulatory action, civil or criminal violations could result from disclosure. It could also cause significant harm to Institutional Information, major impairment to the Location's overall operation, or the impairment of essential service(s). This impact level also includes lower-level impact items that, when combined, represent an increased impact. A security incident is severity "high" if any of the following characteristics are present:

1. Threatens to impact (or does impact) systems critical to the University's ability to function normally. This includes but is not limited to email, courseware, human resources, financials, internet connectivity, or portions of the campus network.
2. It poses a serious threat of financial risk, reputational damage or legal liability.
3. Threatens to expose (or does expose) a significant amount of Level 3 or Level 4 data as defined by the Data Classification Standard.
4. Significant threat to propagate to or attack other networks or organizations internal or external to the University.
5. Terroristic threats or other threats to human life or property.

Medium:

Unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could: (a) result in moderate damage to UofT, its students, employees, community or reputation; (b) result in moderate financial loss; or (c) require legal action. This impact level also includes lower-level impact items that, when combined, represent an increased impact. A security incident is severity "medium" if any of the following characteristics are present:

1. Threatens to impact (or does impact) a significant number of systems or people. The University can still function, but a group, department, Unit, or building may not be able to perform its mission.
2. Systems impacted may contain any level of data as defined by the data classification standard; however, only a limited amount of Level 3 or Level 4 data.
3. Moderate threat to propagate to or attack other networks or organizations internal or external to the University.

Low:

Unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in minor damage, small financial loss or affect the privacy of an individual or small group. Low severity incidents tend to have routine solutions and have no characteristics from the "medium" or "high" categories and may include the following:

1. It impacts only a small number of people or systems.
2. Impacted systems contain a limited amount of only Level 1 or Level 2 data or a minimal amount of Level 3 data as defined by the data classification standard.
3. Little to no risk of the incident spreading or impacting other organizations or networks.

Appendix C contains a Heat Map to aid in the determination of the severity category as required.

5.0 Computer Security Incident Response Team (CSIRT)

Given the federated nature of the University, there may be two main models to organize the incident response teams:

Unit Incident Response Team – Units need to have staff and resources identified to manage security incidents on behalf of that Unit. Among other things, they will perform analysis, investigation, and coordination of activities for the Unit to contain and remediate risks derived from security incidents. They will act solely on behalf of a particular Unit and within the boundaries of their own Incident Response Plan. Unit Incident Response Team will be formed for most low severity incidents.

Institutional Computer Security Incident Response Team (CSIRT) - The CSIRT is a cross-functional team dedicated to managing security incidents on behalf of the University. It will coordinate various resources during the incident. The CISRT comprises members from both the affected Unit and institutional university departments. These are the people actively working on the incident and led by the incident manager. Among other things, they will perform analysis, investigation, and coordination of activities for multiple constituencies to contain and remediate risks derived from security incidents.

The CSIRT will be formed mostly to respond to medium and high-severity incidents. However, it may be called for resolution of non-routine low severity incidents as well.

As part of CSIRT, there are permanent and ad-hoc members who are engaged depending on the incident's needs.

The CSIRT team will act on behalf of Units if they do not have an in-place incident response team structure within the Incident Response Plan's boundaries.

5.1 CSIRT Activation

The following are the criteria for activation of the CSIRT

Severity	CSIRT Activation Criteria
High	There will always be a CSIRT associated with High Severity incidents
Medium	A CSIRT might be activated upon the request of the Chief Information Security Officer (CISO). It is discretionary, and it depends on the merit of the incident
Low	For low severity incidents, a CSIRT may be activated for non-routine incidents and upon the request of the Incident response team

5.2 CSIRT Membership

In general, the team comprises one or more members from the following types of staff depending on the severity of the incident:

Role	Function	Tenure	Responsibilities
Incident Manager	Management	Permanent	Coordinate incident response activities with internal and external stakeholders to the University and leads the Incident Response.
Associate Director, Information Security Operations (ISEA, IT&S)	Management	Ad-hoc (Mostly engaged on Medium/High Severity Incidents)	Point of escalation on security incidents. The Associate Director may assist the Incident Manager with communication efforts or other coordination activities.
CISO	Management	Ad-hoc (Mostly engaged on High Severity Incidents and certain kinds of medium severity incidents)	The CISO may provide authorization to disconnect critical and high visibility systems if they pose a significant reputational, financial or operational risk to the University.
Division/Department/ Faculty Manager	Management	Permanent	Provides coordination of internal faculty resources to aid in the resolution of the incident.
Information Security	Investigator	Permanent	Conduct investigations on security incidents leveraging multiple detective and investigative tools.
Technical Subject Matter Experts (SME) familiar with the	Investigator	Ad-hoc (Mostly engaged on Medium/High Severity Incidents)	Aids in containing, mitigating the impact of and recovering from the incident.

environment and applications			Collects evidence and relevant information to aid in the investigation.
Third-Party forensics firm staff	Investigator	Ad-hoc (Mostly engaged on High Severity Incidents)	Perform in-depth investigations on the cause of incidents, the extent of the compromise, the likelihood of data exfiltration, lateral movement or any other effects of cyber-attacks.
Divisional/Departmental/Faculty Information Security or IT	Investigator	Permanent	Provide necessary evidence in the investigation of security incidents. The team will also perform tasks required to mitigate the impact and risks related to the incident.
Campus Police	Legal	Ad-hoc (Mostly engaged on certain kinds of High Severity Incidents)	May be engaged at times to investigate security incidents and enforce the University of Toronto Student Code of Conduct
Freedom of Information and Protection of Privacy (FIPP)	Legal	Ad-hoc (Mostly engaged on High Severity Incidents and certain kinds of medium severity incidents)	Provides advice on protecting the privacy of students, staff and faculty of the University of Toronto and how to address breaches of their privacy.
Legal Counsel	Legal	Ad-hoc (Mostly engaged on High Severity Incidents and certain kinds of medium severity incidents)	Provide advice on legal obligations emanating from incidents that impact the University of Toronto.
Human Resources	Business	Ad-hoc (Mostly engaged on certain kinds of High Severity Incidents)	Provide advice on personnel matters arising from impacts of certain security incidents.
Communications	Business	Ad-hoc (Mostly engaged on certain kinds of High Severity Incidents)	Provide liaison and external communication services for incidents that may significantly impact the University's reputation.
Applications or data owners	Business	Permanent	Provide business leadership and support in the resolution of security incidents impacting their respective applications or data.

The list above is not exhaustive and other members not listed may be added if they need to be involved or bring value to the investigation or response.

5.3 Meetings

An initial meeting of the CSIRT shall happen as quickly as possible. In all likelihood, this may happen before all the details about the incident are available but will ensure that everyone understands what is happening and what their role is.

Depending on the severity, daily meetings are typically better to ensures good communication and instills the sense of urgency needed to remediate the incident quickly. Working to people's schedules is ideal; a Security incident takes priority over most things, so be aware you will not find perfect meeting times each day. It is better to be consistent and schedule meetings where people can provide the best new information, typically late morning or afternoon.

5.4 Communication

Wherever possible, it is essential to keep all (or as much as possible) communication in one place. Incident Response Teams shall set up private channels of conversation if the scope and severity warrant it where discussions about the incident and artifacts from the investigation can be kept in one place. Launching meetings from this channel also ensures that information in the chat for those meetings also stays in the same place.

These procedures would need to work by bringing in each necessary key area and would also leverage more detailed response/work plans in each of those areas.

Additionally, officials from any area; Faculty, other divisions, departments, etc., affected by an incident would need to be fully involved. This is not only as part of the response and possible remediation but also because of local leaders' responsibility for these actions, the results of an incident, and because local leaders might likely control many resources necessary for responses.

Each key area would need to develop its own detailed response/work plan, as should each Division (at a minimum).

Divisions/Departments, etc., responsible for sensitive and/or extensive data holdings should have particularly well-developed plans, proportionate and responsive to the risk associated with the data holdings.

Procedures could comprise at least the following components, depending on the nature of the incident—first for incident response, then for subsequent steps, and each of these components would have several steps/parts:

- Detection/reporting
- Assessment
- Containment
- Documentation

- Briefing Notification
- Standards check/update
- Remediation
- Training
- Process/system redesign
- Assess the efficacy of remediation

6.0 Methodology

This plan outlines the most general tasks for Incident Response. It will be supplemented by specific internal guidelines and procedures that describe the use of security tools and communication channels. These internal guidelines and procedures are subject to amendment as technology changes. It is assumed that these guidelines will be documented in detail and kept up-to-date.

6.1 Incident Response Process

In addition to documenting procedures, all Information Technology managers shall become familiarized with the incident response process to recognize and report incidents as quickly as possible. All faculty and staff are encouraged to report suspected information security incidents as quickly as possible.

Incident Management guidelines and supporting Incident Management (IM) toolkit is provided below:

- Toolkit - IM – Response Guide
- Toolkit - IM - Leadership Summary
- Toolkit - IM - Email Leadership Summary
- Toolkit - IM - Manager Activity Tracking - Sample
- Toolkit - IM - Technical Investigation Report
- Toolkit - IM - Checklist of significant steps for Incident Response and Handling (Appendix D.)

6.2 Incident Identification

The Information Security department maintains and utilizes several tools that scan the University's environment and network traffic, looking for threats. Depending on the severity of found threats or vulnerabilities, they may warn affected users, disconnect affected machines, or apply other mitigations. In the absence of indications of sensitive data exposure, the information security department communicates vulnerabilities to the network/IP owner identified in the IPAM database (http://ipam.utoronto.ca/) and pursues available technology remedies to reduce that risk.

Additionally, the University at large may identify and report suspicious activities, adverse events, or running malicious code. The affected Unit may call an incident on their own or may work with Information Security to formalize the incident if required.

6.3 Containment of the incident and preservation of evidence

Where any data or other artifacts are collected in the investigation, it is imperative to retain those for forensic review and establish a chain of custody. This evidence might be used in litigation should it become necessary.

6.4 Communication Plan and Prioritization

All units shall make the first attempt in classifying incidents according to the severity matrix listed in previous sections of this plan. If incidents are deemed medium or high severity, they need to be reported to the Institutional Security Response Team (security.response@utoronto.ca.) for awareness, assistance and/or escalation to the CISO. The Insititutional Team can also assist in the classification of the incident if required.

Incident Response teams shall document their guidelines for interactions with stakeholders regarding incidents and prioritize incidents with the highest severity level. During incident handling, the organization will need to communicate with multiple stakeholders. Because these communications often need to occur quickly, Incident Response teams shall predetermine communication guidelines.

The incident manager will typically have the responsibility to handle communications as part of the incident response process. In case a CSIRT was established to handle a particular incident, the incident manager will prepare the communication in coordination with the team and target the appropriate audience. The workflow and table are below.

A communication workflow is found on Appendix F

Incident Severity	Target Response Time*	Incident Manager	Who to notify?	Incident Reporting Required?
High	Immediate	IT Security Officer or Delegate	• IT Security Officer • IT Administrator • Unit administrator • Unit Representative • CIO • CISO • Privacy Officer • Institutional Incident Response team • Others on a need-to-know basis	Yes (daily emails informing progress, formal incident report upon closure, lessons learned report)
Medium	4 hours	IT Security Officer or Incident Response Lead	• IT Security Officer • IT Administrator • Unit Representative • CISO • Institutional Incident Response team • Privacy Officer	If requested by IT Security Officer, CIO, or another administrator (Ad-hoc emails informing progress and/or formal

			• Others on a need-to-know basis	incident report or lessons learned report)
Low	As soon as practicable (No more than one business day)	Incident Response Lead	• Unit Representative • Others on a need-to-know basis	(Ad-hoc emails informing progress)

*It refers to the time it would take for the incident response team to respond to incidents.

6.5 Role Equivalency Table (Institutional X Units)

Role	Institutional Teams	Divisional (Unit) Teams
Information Security Officer	• Associate Director, Information Security Operations	• Division, Information Security Lead • Division, IT Manager • Division, IT Leader or delegate
Incident Response Lead	• Incident Response Architect • Security Analyst	• Division, Information Security Lead • Division, IT Manager • Division, IT Leader or delegate
IT Administrator	• N/A	• Division, IT Director • Division, IT Manager • Division, IT Leader or delegate
Unit Administrator	• N/A	• Division, CAO • Division, Dean, Associate Dean • Division, Business Manager or delegate

Unit Representative	• N/A	• Division, Business Manager or delegate
CIO	• CIO or delegate	• N/A
CISO	• CISO or delegate	• N/A
Institutional Incident Response Team	• Institutional Incident Response Team	• N/A
Privacy Officer	• FIPPA Office	• FOIL (Freedom of Information Liaison)
Others on a need-to-know basis	• Institutional IT teams' representatives • Any other relevant person to inform or resolve the incident.	• Other IT teams' representatives • Any other relevant person to inform or resolve the incident.

6.6 Common Incident Types

The Incident Response program's primary objective is to mitigate and contain the risk associated with computer security incidents. Some of the most common types of incidents are:

- Phishing attacks,
- Malware and viruses,
- Denial of resources or services,
- Unauthorized access or attempts to gain unauthorized access,
- Inappropriate use of network resources,
- Ransomware
- Data breaches
- Changes to system hardware, firmware or software without owner's knowledge,
- Any other unlawful activity involving computer networks and processing equipment.

6.7 Playbooks

Following the list of common incident types, playbooks are generally created to handle security incidents systematically and consistently. Incident response teams should leverage “Playbooks” as much as possible. Some examples are provided below:

UTM - Ransomware playbook

Appendix A and Appendix B contain more detailed information on common incidents and examples of how to handle them.

6.8 Training, Awareness & Annual Assessment

General security incident response training, awareness and practices that shall be followed by Units:

- Review and adopt the Incident Response Plan (this document) or use it to create your own plans.
- Familiarize with the methodologies associated with the incident response process, including incident containment and playbooks.
- Review plans once a year and train team members as appropriate for operational readiness.
- Submit incident response plans to be incorporated in the DAI-IRSA annual assessment process.

Incident Response Handling (Practical Guide)

a. Review checklists and toolkits
b. CSIRT
c. Communication Plan
d. Incident Reporting
e. Tabletop Exercises

In addition to documenting procedures, units shall provide training and awareness to staff and faculty to recognize and report incidents as quickly as possible.

UTM Sample InfoSec awareness plan (Example):

UTM - Infosec Awareness Plan

6.9 Reporting an Incident

When reporting an incident to information Security, follow the procedure detailed on the page linked below:

IRP Main Web Page

6.10 Additional External Resources

External resources may be required depending on the severity of the incident and the data types or assets involved. The engagement of those resources would typically incur additional costs to the Unit. These may include:

Breach Coach	A breach Coach is functionally a project manager for an incident. For significantly extensive or severe incidents, the services of a Breach Coach may be needed. In addition to project incident management services, they can also arrange access to the other resources listed below. In many cases, the breach coach role can be subsumed by sufficiently expert external counsel, who can offer breach coaching services/functions as part of their legal advice and guidance.
Credit monitoring services	Where a threat of identity theft is possible for one or many people, the Unit may need to offer identity theft protection insurance to those people. At a minimum, any breaches involving SIN numbers are typically the low watermark for this, but this may still need to be offered if there is enough other personal data involved. The offer to the affected individual is typically for an enrollment period of three months, with coverage provided for a year.
Specialized Legal Counsel	Where large breaches of data have occurred, or there is a threat of legal challenges against the University due to the breach, it may be necessary to engage Specialized Legal Counsel. These specialists are often more experienced with issues and challenges posed by a security incident than the University's General Counsel may be.
Forensic Analysis Firm	A forensic analysis firm provides specialized investigators to review the devices and systems involved in an incident. They will attempt to determine the root cause of the incident, the attackers' activities after they gained access, and what, if any, data was exfiltrated and how it happened. Forensic analysis can be a costly proposition, so ideally, internal staff, assuming they have the skills to do so, will independently investigate the devices and systems involved first. This internal review serves to either mitigate the need for Forensic Analysis or limit the scope to a minimal number of devices and systems. The University has entered into a contract with a Forensic Analysis Firm to limit the cost involved as much as possible. Information Security can help arrange this service for a Unit should it become necessary.

6.11 Tabletop exercises

Institutional and Unit incident response teams shall regularly organize tabletop exercises with several key operational areas and run through exercises to regularly test, develop, and refine incident response procedures, materials, and skills.

As part of the exercises, divisions/departments/faculties responsible for conducting or involving information security investigations shall actively participate when requested.

Additionally, other IT professionals at the University may be requested to participate as needed.

Table Top Scenario Examples

Table Top Exercise Scenarios and Notes

Appendix A: Examples of security events and what to do

Type of security incident	Next Steps / PROCESS	Who to contact
Phishing – user-provided credentials to a malicious site	Reset password UTORID, UTOCSI, VPN, Local accounts, etc. … - An incident ticket is created (depending on inbound vector – user goes to Service Desk, user calls/e-mails InfoSec personnel, IS contacts with reported credential breach) and assigned to the security queue - The InfoSec team husbands the ticket, with Client Services performing the work. The checklist includes password reset, InfoSec awareness, endpoint setup and remediation.	IS, LOCAL IT Support
Potential fraud	- An incident ticket is created (depending on the inbound vector), and Information Security Incident Management Checklist is spawned - The checklist is followed (as per attached), Campus Police husband the process, IT side is coordinated by I&ITS InfoSec team, with IS	
Accidental Information Disclosure	- Report of lost/stolen/compromised sensitive information is received by IT (inbound vector can be the user, other I&ITS team, or our FOIL) - An incident ticket is created, and Information Security Incident Management Checklist is spawned - The checklist is followed (as per attached) including response team assembly, FOIL involvement)	
Compromised device	- An incident ticket is created (depending on inbound vector, user report, Netflow alert, SCEP alert, Palo Alto alert, etc.)	

	- Endpoint recon coordinated by IT team with SMEs from other teams (Classroom Technology, Network Engineering, System Administrators, etc.) - Remove from network - Remediate/reconfigure/reconnect	
➢ MORE ITEMS WILL BE ADDED (Computer Malware, crypto locker, theft of equipment,		

Appendix B: Detailed Examples of Common Incident Types

Compromised credentials

- Phishing: you have inadvertently provided your credentials to a malicious site
- Ransomware and viruses: your computer has been compromised or encrypted by malware or crypto locker
- Potential fraud using misrepresentation of identity, stolen credentials or falsifying identification. Disclosure of credentials through compromised third-party cloud services

Disruption of service, system or device

- Unauthorized access to your computer or your institutional on-line services
- Discovery of installed malware to enable back door access, take ownership over a device, etc.
- Targeted attacks towards specific devices, network resources, or a system

Loss or theft of equipment, including paper records

- Loss of USB key with sensitive, confidential or protected data
- Loss or theft of an unencrypted laptop containing secure data
- Loss of a mobile device or removable media secure data
- Data theft related to a Break-in
- Loss or inappropriate disposal of paper records

Data breaches involving confidential and protected data, including accidental information disclosure

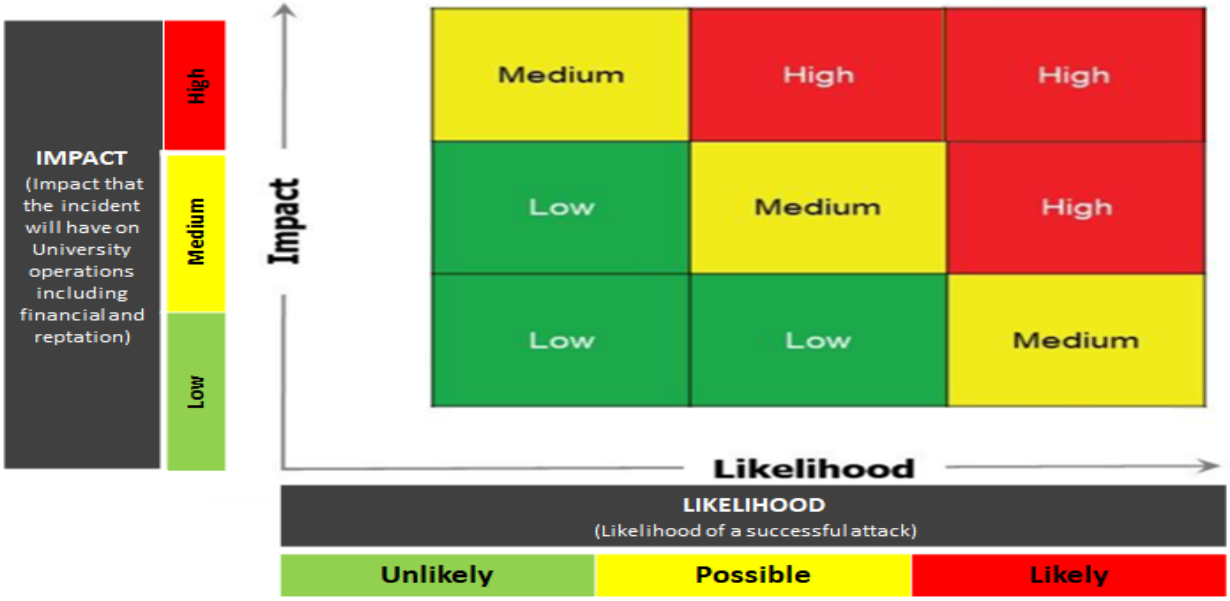
- Protected student information
- Protected health and human subject information
- Payment card information (PCI)
- Personal health information (PHIPA)
- Research information covered by IP or contractual obligations

Improper/unlawful use of information resources or attempts to disrupt the business of the University

- Denial of service attacks. For example, Denial of service attack targeting individual email account(s), causing spam email flood
- Web site defacement or compromise
- Improper system usage, including unlawful use, impersonation, electronic harassment

Appendix C: Severity Ratings – Heat Map

Severity Heat Map:



The severity heat map guides the severity classification of security incidents from a likelihood/impact perspective. This is appropriate given that, in most cases, the impact of incidents is better understood as the investigations evolve and more information becomes available.

TABLE			
Severity	Data Sensitivity	Scope	Description
High	Significant amount of Level 3 or Level 4 data	Institutionally Significant	Significant fines, penalties, regulatory action, civil or criminal violations could result from disclosure. It could also cause significant harm to Institutional Information, major impairment to the overall operation of the Location or the impairment of essential service(s).
Medium	Limited amount of level 3 or Level 4 data	Faculty or Business Significant	Unauthorized use, access, disclosure, acquisition, modification, loss or deletion could: (a) result in moderate damage to UofT, its students, employees, community or reputation; (b) result in moderate financial loss; or (c) make legal action necessary.
Low	Limited amount of level 1, level 2 or level 3 data	Individual or Group	Unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in minor damage, small financial loss or affect the privacy of an individual or small group.

Please see the Data Classification Standard

To make an initial determination of the severity of an incident, the Incident Response team shall first assess the incident's **potentia**l impact:

IMPACT (Impact that the incident will have on University operations including financial and reptation)	**High**	Highly sensitive data was exfiltrated, changed, deleted, or otherwise compromised. Successful propagation or attack against other networks or organizations internal or external to the University. The University is no longer able to provide some critical services to any users as a result of an attack.
	Medium	Limited amount of sensitive data was exfiltrated, changed, deleted, or otherwise compromised. Limited success in propagation or attack against other networks or organizations internal or external to the University. The University has lost the ability to provide a critical service to a subset of system users as a result of an attack.
	Low	Non-sensitive data was exfiltrated, changed, deleted, or otherwise compromised. Minimal effect; the University can still provide all critical services to all users but has lost efficiency.

Once the potential impact is determined, the incident response team shall make a judgement on the likelihood. Once potential impact and likelihood are established, these are plotted against the Severity Heat Map to define a Severity rating.

LIKELIHOOD (Likelihood of a successful attack)	**Likely**	There is high probability of data exfiltration or lateral movement of cyber attacks as a result of indications from visibility tools or analysis performed by the investigating teams.
	Possible	There is moderate probability of data exfiltration or lateral movement of cyber attacks as a result of indications from visibility tools, analysis performed by the investigating teams. This option can also be chosen if there is no clear indication of successful attempts of an attack.
	Unlikely	There is low probability of data exfiltration or lateral movement of cyber attacks as a result of indications from visibility tools or analysis performed by the investigating teams.

The low/medium/high scale gives a qualitative dimension to articulate severity. For example, a security incident deemed with Low Likelihood and Low Impact would be categorized as Low Severity. In contrast, an incident deemed High Impact/High Likelihood would be identified as High Severity.

Once investigations conclude, the security incident severity is equated to the known impact against the severity categories. If the impact remains unclear, the severity shall be determined from a likelihood/impact perspective.

Appendix D: Checklist of significant steps for Incident Response and Handling

a. Preparation — Includes documentation, testing, training and other preparatory activities.

- ❑ Review and adopt the University Incident response plan, or use it to create your own.
- ❑ Create a prioritized list of critical information assets to the functioning of your Unit.
- ❑ Ensure a communication plan is in place for each severity of the incident.
- ❑ Identify who will be on the CSIRT team; this can be specific people or identified positions.
- ❑ Identify any tools needed for communication, artifact collection, or other activities.
- ❑ Document as much as possible ahead of time and ensure that the files are somewhere it will be available when needed.
- ❑ Train staff or faculty on how to identify an incident and how to report it. The CSIRT team members run a tabletop exercise to understand their role and responsibilities in the process.
- ❑ If available, identify and review the Unit's IT and Business Continuity Plans
- ❑ Review the plan and documentation annually to ensure it stays up to date.

b. Identification —This identifies what data, devices, or systems were damaged, accessed, or exposed as part of the breach. Additionally includes the collection of logs, system images, and other artifacts. Activation of the CSIRT happens at this time.

- ❑ Understand what has happened, what assets are affected, and the overall impact
- ❑ Begin documenting the incident timeline, any actions taken, and artifacts collected. This may be the best estimate for the timeline, as details may not be available at this point.
- ❑ Classify the data and criticality of impacted assets
- ❑ Determine the severity of the incident
- ❑ Assemble a Security Incident Response Team (CSIRT) and assign an Incident Manager
- ❑ Activate the communication channels needed for the CSIRT team and others that must be notified.
- ❑ Determine if a breach coach or external forensics is needed
- ❑ Collect Logs related to the event. These include but are not limited to those from:
- ❑ Network devices
- ❑ Centralized logging (SIEM, Syslog Servers)
- ❑ Authentication sources (LDAP, Active Directory, RADIUS, etc.)

c. Containment — Initial short-term containment of the incident, primarily this will be disconnecting devices or networks to limit any spread of malware or malicious activity. Start Short-term containment to stop the attack/issue. This includes:

- ❑ Isolate affected assets – disconnect from the network but do not power off!
- ❑ If available, take the appropriate measures to restore services according to the Unit's IT and Business Continuity Plans.
- ❑ Assess risk to other systems
- ❑ Apply additional interim mitigations, additions to monitoring, etc.
- ❑ Collect evidence for additional review, and any possible legal proceedings
- ❑ Create forensics images of the hard drives and memory
- ❑ Take a snapshot of Virtual machines to preserve the current state.
- ❑ Retrieve hard copies of any disclosed personal information.
- ❑ Continue to document findings
- ❑ Report results to CSIRT

d. Eradication— Identify the root cause of the incident. Remove malware, malicious code and vulnerabilities from all affected systems using the identification step's collected information.

- ❑ Identify the root cause — It's critical to understand what caused the incident to prevent future compromises for the same reason.
- ❑ Scan for malware — use anti-malware software or Next-Generation Antivirus (NGAV) if available to help determine the root cause.
- ❑ Restore, Rebuild, or Replace — A compromised system shall never be cleaned and restored to production unless there is no other option.
- ❑ Restoring a system from backup can be an effective method to get a system back into production quickly; however, any backups used must be from before the compromise occurred.
- ❑ Rebuilding a system from scratch is more time-consuming but ensures a clean system.
- ❑ Replacing an old system with newer versions of the OS and applications is more time-consuming but effective to ensure a system is up to date and secure.

e. Recovery — Return systems carefully back to production status, ensuring mitigation of the root cause occurs first.

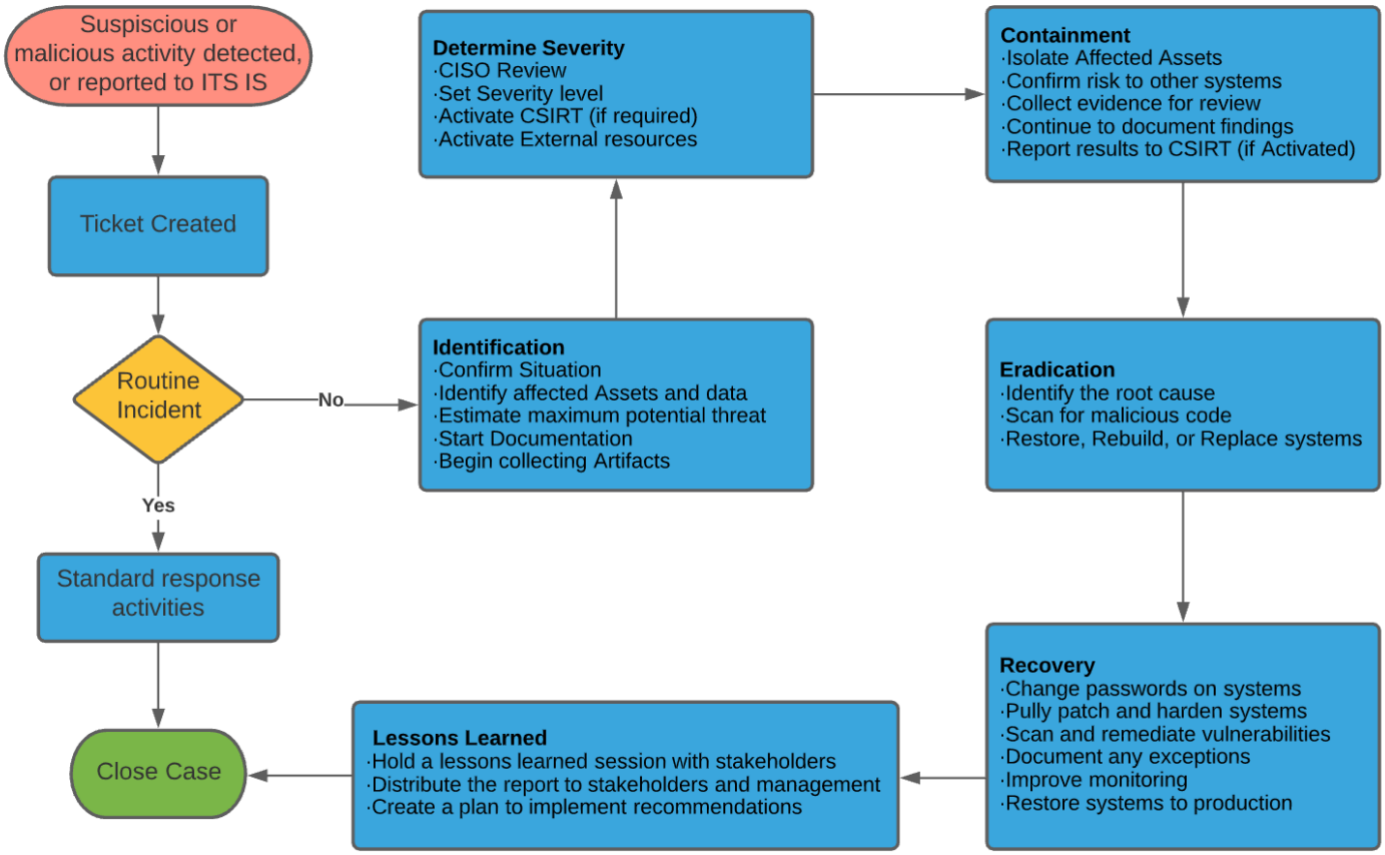
- ❑ Fully patch all systems before connecting to the network.
- ❑ Change all local system and user passwords on affected systems before redeployment. This activity shall extend to any centralized accounts that used the system as well.
- ❑ All passwords and private keys stored on the system used to access other systems must be changed.
- ❑ Harden a system to a well-documented standard. (i.e. CIS Benchmarks)
- ❑ Scan for and remediate discovered vulnerabilities before redeployment.
- ❑ Document any exceptions for vulnerabilities that cannot be remediated, including the compensating controls used instead.
- ❑ Improve monitoring to help stop any recurrence of the incident.

f. Lessons learned — Review the root cause of the incident and identify opportunities to improve detection and defences to lessen a reoccurrence chance. Also, review the process of dealing with the incident and determine any improvements there as well.

- ❑ Hold a lessons learned session with stakeholders and CSIRT members to identify opportunities to improve detection of malicious activity, defences, and the incident response process.
- ❑ Create a report based on that session's results with the issues identified and recommendations for improvement. Ensure management views the report if they were not involved with the lessons learned session.
- ❑ Create a plan to implement any recommended changes and improvements with target dates for completion.

Appendix E: Generalized cyber incident escalation and workflow diagram

The following is a workflow diagram for a generic incident. Do not use this as a strict workflow as several incident stages may be in process all at once.

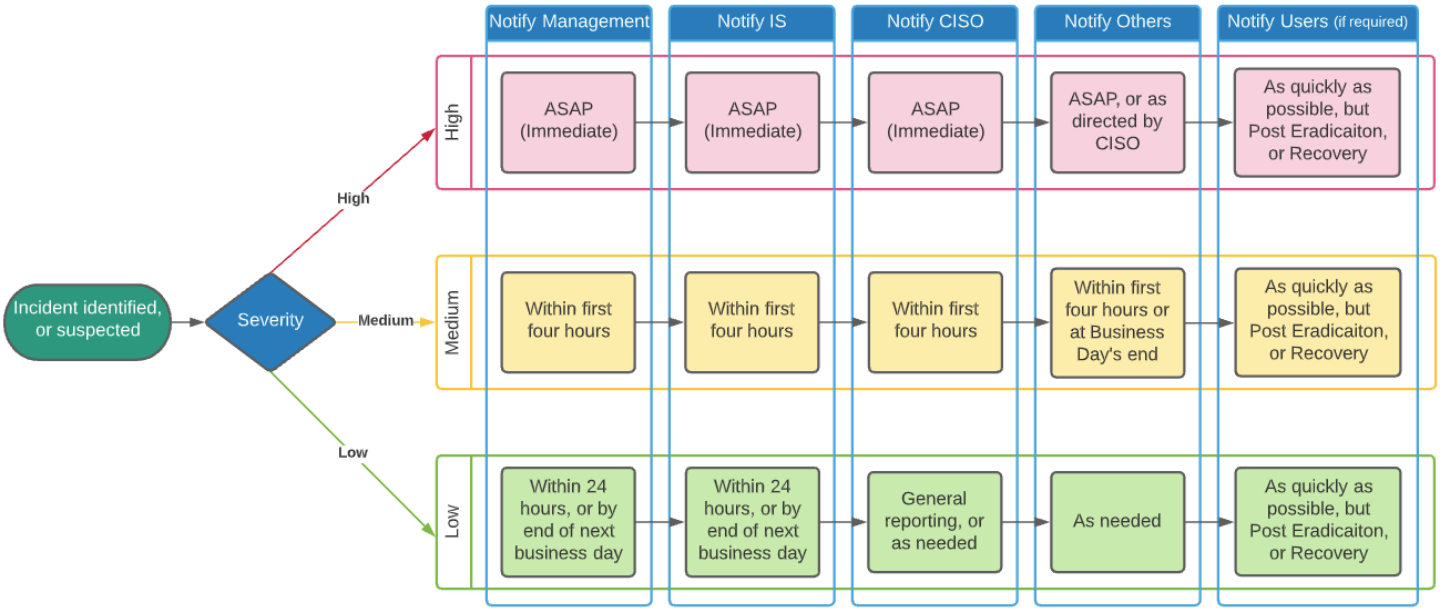


Appendix F: Cyber incident notification workflow diagram

The following is a notification and escalation workflow showing the ideal timeframes that specific parties shall be made aware of an incident. Ideally, notification and escalation shall happen as soon as possible to ensure that an incident receives the support it needs as quickly as possible.

Notify	Meaning*
Management	Unit Administrator, IT Administrator, Unit Representative
IS	Information Security at Local unit, and/or Cental
CISO	University Chief Information Security Officer.
Others	CIO, Privacy Officer, Communications, Legal Counsel, Law enforcement, IMG.
Users	Anyone whose personal data may have been exposed in some way.

*See section Role Equivalency Table (Institutional X Units) for more information



Appendix G: References

- NIST - Computer Security Incident Response Guide (SP 800-61 Rev. 2)
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- Carnegie Mellon University - Incident Response Plan
  https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf

- eHealth Ontario - Electronic Health Record Privacy Incidents & Privacy Breaches Policy
  https://www.ehealthontario.on.ca/images/uploads/pages/documents/PHI_PrivacyPolicy_EN.pdf

- The University of British Columbia – Incident Response Plan
  https://it.ubc.ca/sites/it.ubc.ca/files/UBC_Incident_Response_Plan7600.pdf

- Western Oregon University – Data Security Breach Incident Response Plan
  https://www.wou.edu/ucs/policy/WOU_Incident_Resp_Plan.pdf

- The University of Waterloo - Computer security incident response procedure
  https://uwaterloo.ca/information-systems-technology/about/policies-standards-and-guidelines/security/incident-response-procedure#Responder

- The University of Waterloo - Information Security Breach Response Procedure
  https://uwaterloo.ca/secretariat/information-and-privacy/information-security-breach-response-procedure

- Stanford University - Information Security Incident Response
  https://adminguide.stanford.edu/chapter-6/subchapter-6/policy-6-6-1

- Virginia Tech Guide for Cyber Security Incident Response – A very well written plan
  https://security.vt.edu/content/dam/security_vt_edu/downloads/incident_response.pdf

- University of Toronto – Crisis and Routine Emergency Preparedness and Response, Policy
  https://governingcouncil.utoronto.ca/secretariat/policies/crisis-and-routine-emergency-preparedness-and-response-policy-june-27-2018

Appendix H: Changelog

Date	Version	Change	Made by
19 January 2021	0.2	A significant document revamp with changes to content in every section.	Deyves Fonseca, Alex Tichine, Andrew Wagg
2 February 2021	0.3	Small changes to multiple sections; larger changes are: • Severity heat map clarified and expanded • Addition of a changelog • Expanded Incident Response Process	Deyves Fonseca, Andrew Wagg
9 February 2021	0.4	Small changes to multiple sections; larger changes are: • Moved Incident Response process to its own section (3) • Updated Toolkit - IM- Response Guide to match Incident Response process • Added content to Appendixes d, and E	Deyves Fonseca, Alex Tichine, Andrew Wagg
11 February 2021		Update introduction to remove duplication of incident types and consolidated objective of the plan.	Alex Tichine
18 February 2021		Update to the classification of impact from minor, moderate, major to low, medium, high.	Deyves Fonseca
19 February 2021		Respond to comments and document polish.	Deyves Fonseca, Alex Tichine, Andrew Wagg
23 February 2021		Small changes to multiple sections; larger changes are: • Added Appendix F: Cyber incident notification workflow diagram	Isaac Straley, Deyves Fonseca, Alex Tichine, Andrew Wagg
23 February 2021		Minor update of section 6.4 to make it clear the role of Incident Manager in communications. Updated section 6.8 to include annual assessment and Clarifications on language related to responsibilities.	Deyves Fonseca