POLICY TITLE:	**Cyber Security Incident Management Policy**
APPROVED BY / DATE:	**Robert Devries, CIO – September 14, 2023**
Last Revised Date:	**August 18, 2023**
Next Review Date:	One year after Approval
Brief Description:	This Policy defines a standard University-wide process for managing preparations for and response to information security incidents.

Table of Contents

Introduction

This Policy defines a standard University-wide process for mitigating risk of information security incidents in advance of their occurrence and provides guidance for initiating a rapid response and the appropriate escalation when a Major information security incident (see "Information Security Incidents Defined") occurs or is suspected to have occurred.

This Policy charters a standby Cyber Security Incident Response Team (CSIRT). The University Chief Information Officer (CIO) is the executive sponsor of this policy and the CSIRT. The Cyber Security Incident Response Process (Appendix A) documents the conditions under which the CSIRT will be activated and how University leadership, Campus Safety Office, and other stakeholders are involved. This policy also references the University's Emergency Management Plan which details responsibilities for campus emergency situations or disruptions.

Scope

This policy applies to all University of Guelph students, staff, faculty and contractors, and all information technology systems, services, data and infrastructure owned by or operated for the University, including cloud-based and managed services.

The policy is applicable to information security incidents that are categorized as either Major or Significant and which affect U of G-operated and/or U of G-owned IT facilities, infrastructure, assets, services, data sets and community stakeholders.

All University of Guelph faculty, staff, students and contractors are guided by the Acceptable Use Policy for Information Technology (AUP) for minor IT-related security incidents. The AUP specifies the responsibilities of individual users, system administrators, information technology (IT) service providers and management with regard to the utilization of University IT services and resources. The AUP also specifies the complaint and resolution process for alleged acceptable use violations.

Objectives

This incident response policy enables the University to respond to Major information security incidents in an efficient, coordinated, appropriate, and cost-effective manner that:

- identifies accountability for responding to an information security incident and ensures appropriate escalation when required,
- avoids or minimizes service outages for University systems and applications that may result from a security incident,
- streamlines the response process and restores services in an expedited manner,
- avoids or minimizes damage to individuals whose personally identifiable information (PII) or personal health information (PHI) may have been compromised,
- secures and protects data and other information technology services/assets in order to minimize the organizational impacts such as short and long-term financial loss, reputational impact, regulatory impact and business losses resulting from a security incident, and
- minimizes the risk and likelihood of a similar incident occurring in the future.

Policy Statements

1. This Policy defines information security incidents and their categorization, a standard process for managing incidents, and specifies individual responsibilities including the protocol for incident reporting, resolution, and closure.
2. This Policy establishes a stand-by Cyber Security Incident Response Team (CSIRT) which will be invoked as required by the CIO, Chief Information Security Officer (CISO) or assigned designate.
3. The CSIRT will manage and support incident response activities, including communication, remediation, escalation, and closure.
4. The CSIRT will enlist and assign technical resources as required to conduct immediate investigation of the sources or causes of major incidents. This could include both CCS and distributed IT resources.
5. When criminal activity is alleged or suspected, the Campus Safety Office must be engaged by the CSIRT.
6. When unauthorized disclosure of sensitive/confidential data or personally identifiable information (PII) or personal health information (PHI) is alleged or suspected, the University Secretariat must be engaged by the CSIRT.
7. In situations where there is a financial impact to the University, or financial systems are involved in an incident, such as in the case of financial fraud, the Chief Internal Auditor and the VP Finance Administration & Risk must be engaged by the CSIRT.
8. In the event of a Significant or Major incident, the CISO or CIO will engage the Provost, the President, Office of Legal Counsel and other members of the University executive leadership team regarding the potential of declaring an emergency and activating the University's Emergency Management Plan.
9. This Policy authorizes the CISO, in coordination with the CIO, to assign resources, which may include staff and/or financial resources, to apply the best available remediation strategies in response to a security incident. This includes but is not limited to the introduction of new security controls or processes for university resources. As an outcome of a security incident, it may be necessary to assign additional resources to take corrective or proactive action to prevent future security incidents.
10. The CISO, in coordination with the CSIRT and Treasury Operations, will determine if engaging the University's cyber security insurance provider is required by the terms of our insurance policy or necessary to provide additional resources for containment, recovery, or forensic investigation. Timing of notification to the insurance provider will be consistent with the insurance policy requirements.
11. As mandated by the Ontario Ministry of Colleges and Universities, the CISO will initiate communication with the University of Guelph Government Relations and Community Engagement team to report the incident to the Ministry in the event that there is a potential that it will impact the broader Ontario Public Sector, or if the incident has attracted, or has a high likelihood of attracting media attention.
12. The CISO will coordinate with the University Secretariat to determine if notification to the Information and Privacy Commissioner of Ontario (IPC) is necessary.
13. As a member of the Canadian higher education community, the CISO is authorized to share cyber attack information and indicators of compromise (IOCs) with the Canadian Shared Security Operations Centre (CanSSOC), REN-ISAC, other higher education security partners, the Canadian Centre for Cyber Security (CCCS), and other law enforcement

agencies as soon as possible to aid in the protection other institutions. Information must be shared without attribution to the University of Guelph and must not contain confidential or privileged information, PII or PHI.

14. As required for response to a major security incident, the CISO has the authority to suspend CCS operational change request and approval process to facilitate rapid response to the incident.
15. CSIRT members and staff involved in the incident response process must maintain strict confidentiality around incident details, and must adhere to guidance provided by the CIO, CISO, Office of Legal Counsel, University Secretariat, and/or University leadership regarding information sharing.

Information Security Incidents Defined

Security incidents will be categorized based on severity:

Severity	Description
Minor Incident	Minor security incidents involve a reported security issue that may impact a single individual, a non-critical system, or a policy violation that does not have a widespread impact and is not criminal in nature. Minor incidents are managed by the Information Security team following standard operation procedures (SOP) and the University of Guelph Acceptable Use Policy for Information Technology (AUP). Examples include, but are not limited to: • Acceptable Use Policy (AUP) violations • Copyright complaints • Compromised non-privileged user accounts • Single non-critical system malware infections where no data breach is suspected • Reports of spam and phishing email messages
Significant Incident	A Significant security incident has greater scope than a minor incident, and involves multiple parties, critical systems, or teams. These incidents have a larger impact or service level disruption on University services or systems, may involve public facing systems, or affect an external organization. These incidents are typically managed by the Information Security team and may require the assistance from other support teams on campus. A Significant incident may be escalated to Major based on the severity, impact and nature of the incident. Examples include, but are not limited to: • Limited distributed denial of service (DDoS) attacks • Compromised administrator credentials • Targeted or high-volume spam or phishing • Data breaches with minimal scope or risk • Malware infection with significant scope or risk
Major Incident	Major information security incidents include, but are not limited to: • Service impacting DDoS attacks on the University network, enterprise application systems or IT infrastructure • Unauthorized access and/or changes to information systems • Theft or misuse of data • Data breaches with significant risk • Criminal acts such as financial fraud • Violations of privacy legislation • Malware or ransomware attacks affecting multiple systems or representing an impact to campus services. • Potential exposure of Confidential (S3) or Restricted (S4) data as defined by the University Data Storage Guideline. • Threats to human life or property

	A significant service level disruption to the University networking infrastructure or any major application system may be escalated to a Major incident if the suspected root cause is security related. Any unauthorized intrusion that impacts the availability or integrity of critical IT services such as email, telephony, collaboration, administrative systems, internet access, or any disruption that affects large numbers of users will be considered a Major security incident. Major security incidents also include enterprise application systems and/or databases that have been compromised by malware, by unauthorized use of administrative accounts, unauthorized disclosure of personal or sensitive information, and either loss or corruption of data. This includes both on-premise and cloud-hosted systems and applications.

Incident Response Phases

A coordinated response to Major information security incidents will progress through the following phases. It is important to note that during an incident, the process steps may not always flow sequentially, and some actions may take place concurrently.

1. **Preparation**
   The Preparation phase covers the work that the University does in order to be ready to respond to an incident. This includes the need for people (resources and training), process (security policy and established procedures), and technology (support for the necessary tools and services for incident detection and response). This phase includes the proactive efforts undertaken to prevent cyber security incidents from happening.

   - Establish and review incident response policies, procedures, playbooks, and communication protocols on an annual basis.
   - As required, identify individuals from applicable units that may be appointed, consulted or engaged by the CSIRT during an incident and provide appropriate training.
   - Conduct annual tabletop exercises to test incident response procedures.
   - Maintain an adequate asset inventory list and identify the most critical assets that require the highest level of protection and will be given the highest priority in the event of an incident.
   - Develop specific recovery plans for the most critical assets.
   - Manage and update the stakeholder list with current communication information.
   - Support and promote the proactive components of the University's information security program within the community, including cyber security awareness training, vulnerability management, and risk assessment for new infrastructure and services.
   - Establish and test backup incident response resources, such as:
     - A document repository containing breach response, playbooks, policies, and contact information outside of the normal day-to-day operational resources.
     - Primary and secondary communication methods for engaging the CSIRT and communicating during an incident.

2. **Discovery, Identification, and Containment**
   When an incident is first discovered or reported, the number of individuals with knowledge of the situation should be contained to a small group. The objective of this phase of the process is to provide initial notification and minimize the impact given the best information available at the time.

   - Initial incident triage.
   - Confirm that an incident has occurred.
   - Contain the incident as much as possible.
   - Invoke the CSIRT if necessary.
   - Investigate to confirm or rule out the existence of a data breach and determine the types of information involved in the incident.
   - Confirm the incident severity level (Minor, Significant, or Major).
   - Where required by policy, notify the necessary University leadership and stakeholders of the incident including the initial findings.
   - University leadership will convene the Emergency Operations Committee (EOC) at this time if deemed necessary.
   - In coordination with the CSIRT, University leadership, and Treasury Operations, the CISO will determine if engaging the University's cyber security insurance

provider for additional assistance from a breach coach or forensics resources is warranted.
- When appropriate, CSIRT or the designated incident communications manager will communicate with IT leaders and/or staff on campus. Communications at this stage will contain minimal information to protect the integrity of the investigation, but may be used to keep staff informed of the situation or to solicit assistance with the containment activities.

3. Investigation and Engagement

The objective of this phase is to conduct a thorough investigation and assessment of the situation to determine next steps.

- An investigation will be performed to determine the circumstances and root cause of the incident, whether the incident has been contained or is ongoing, and what systems, processes, or personnel changes are necessary to help prevent similar incidents in the future.
- The CSIRT is responsible for determining whether any potential legal or privacy impacts. They will then engage University legal counsel and the University Secretariat to formulate mitigation plans and assist in determining any legal responsibilities.
- The CSIRT must determine whether law enforcement should be involved with the incident investigation and document evidence as appropriate. When criminal activity is alleged or suspected, the Campus Safety Office must be engaged.
- In the event that this incident is related to data privacy, the University Secretariat must be engaged. A Privacy Incident Report may be required to be completed by the responsible department or individual.
- In the event that there is a financial impact to the University, or the incident is related to financial systems, the Vice President Finance, Administration & Risk, and the Chief Internal Auditor must be engaged.
- Documentation of findings and evidence must be kept in a shared location available only to the CSIRT and Information Security teams for future reference.
- At this point deidentified indicators of compromise (IOCs) should be shared with the Canadian Shared Security Operations Centre (CanSSOC) and other threat intelligence partners if available.

4. Response

The objective of this phase is to execute on approved recommendations from the investigation including notification, public relations efforts, legal and law enforcement efforts, personnel actions, and system and process changes to help prevent similar issues in the future.

- Providing notification to affected parties will be a coordinated effort between required members of the CSIRT, University Secretariat, Communications and Marketing, Office of Legal Counsel, and any third-party consultants engaged through our cyber security insurance provider. Notification could include direct notification to affected individuals and notification to government or regulatory bodies such as the Information and Privacy Commissioner of Ontario (IPC) and the Ontario Ministry of Colleges and Universities. Coordination and final decision-making authority regarding notification rests with the University Secretary, as Chief Privacy Officer.
- When required by policy, in coordination with Treasury Operations, the CISO will notify the University's cyber security insurance provider of the incident if they are

not already engaged. Specialized public relations assistance from the insurance provider may also be requested at this point.
- Execute on any necessary system or process changes to resolve the incident and prevent repeat incidents.
- When multiple services are impacted, the CSIRT or EOC should establish an order of priority for service restoration. This will assist the technical teams to focus on the most pressing needs of the University first.

5. Closure

The final phase of the incident is closure. The objective is to appropriately close all parts of the investigation, review the process, and communicate findings with the intention of awareness, process improvement, and incident prevention in the future.

- In order to properly close a Major incident, the CSIRT will conduct a post-mortem exercise to review the incident, the actions taken, and the effectiveness of the response to adjust the process for future incidents.
- If requested by University leadership, a full incident report will be written summarizing all phases of the incident, all actions taken, and any lessons learned.
- If any agreed action or remediation cannot be completed prior to closure, Internal Audit should be engaged for tracking purposes.
- A debrief session may also be held with any affected departments to review the incident, raise awareness of the impact, and address any process or technical issues that may have led to the incident.
- Broader university or public communication will occur if deemed necessary by the CIO and University leadership, including but not limited to presentation to the Board of Governors, the Board of Governors Audit and Risk Committee, the IT Campus Leaders Group, and IT staff on campus.
- Transparency is a core principle of the University and every effort will be made to communicate relevant information about any major security incident to stakeholders in a timely manner. However, given the potential financial and reputational impacts of a security incident, the Office of Legal Counsel and the University Secretariat must be consulted prior to any disclosure and communication.

Stakeholders

A Major or Significant information security incident could have broad implications to the University, members of the University community, and other parties that have a relationship with the University of Guelph. The following stakeholders should be considered when managing an incident, specifically with respect to communication.

Primary Stakeholders	Secondary Stakeholders	Other Stakeholders
• Executive Leadership • Emergency Operations Committee (EOC) • Board of Governors • CCS and Campus IT Leaders • University Secretariat • Finance and Risk Management • Campus Safety Office • Office of Legal Counsel • Internal Audit • Communications and Marketing • Government Relations and Community Engagement • Data owners or data custodians	• Students, staff, and faculty • University alumni • University donors • University clients, tenants, and lessees • University or Departmental client groups • Cyber insurance provider(s) • Managed service providers • Provincial and Federal government, including the Ontario Ministry of Colleges and Universities, and the Information and Privacy Commissioner of Ontario (IPC) • Canadian Centre for Cyber Security (CCCS) • City, Provincial, and Federal Law Enforcement	• City of Guelph • Peer higher education institutions • Information Sharing associations (CanSSOC, CUCCIO, REN-ISAC, etc.) • Specialized Security Organizations (Canadian Centre for Cyber Security) • Media • Software Vendors • Internet Service Providers • Owners of attacking infrastructure • Other institutions that the University has partnered with for Information Technology services • Statistics Canada (Branch Research Data Centre) • Healthcare service providers with information sharing agreements with University Student Wellness Services.

Responsibilities

1) All Members of the University Community (including students, staff, faculty, staff, and contractors)

i) Reporting any unusual or suspected improper computer activity, including violations of the AUP, to both the Information Security team (via email at infosec@uoguelph.ca or by contacting the CCS Help Centre 519-824-4120 x58888 or ITHelp@uoguelph.ca) and their immediate supervisor.

2) University IT Staff

i) Reporting any unusual or suspected improper computer activity, security incident or alleged AUP violation simultaneously to their applicable Unit Head/Department Chair and the Information Security team. Suspected criminal activity (e.g. child pornography), or theft of IT assets should be reported directly to University of Guelph Campus Safety Office.
ii) During an incident, avoid making any modifications to systems/equipment involved (or suspected of involvement) until receiving instruction from the CSIRT or Information Security team. Disconnection from the network (where possible) is the recommended first action, however powering off the system or making any other changes should only be done if instructed to do so.
iii) Follow guidelines and direction from the CSIRT and/or Information Security and make the technical asset/resources available from their units as and when requested that includes but not limited to machines from their unit for collecting forensic evidence.

3) Department Chairs/Managers/Unit Heads

i) Ensuring any unusual or suspected improper computer activity, security incident or alleged AUP violation is reported simultaneously to the Information Security team and their applicable Dean/Director.
ii) Ensuring any suspected criminal activity (e.g. child pornography), or theft of IT assets is reported to University of Guelph Campus Safety Office.

4) Information Security

i) Act as the initial CSIRT team until an incident has been classified as Major and the CSIRT team has been formally convened.
ii) Recommend the CISO convene the CSIRT when appropriate.
iii) Categorize, record, and track and document all reports of IT incidents in the centrally managed ticketing system.
iv) Maintain evidence, notes and other incident information in a central location for future reference.

5) Cyber Security Incident Response Team (CSIRT)

i) Follow the CSIRT process as documented in the Cyber Security Incident Response Process (Appendix A).

6) Chief Information Security Officer (CISO)

i) Convene the CSIRT when necessary. In the event the CISO is unavailable, the CSIRT can also be convened by the CIO or an appointed delegate.
ii) Oversee and direct all phases of the CSIRT process.
iii) Report Major and Significant incidents to the Chief Information Officer (CIO).
iv) Coordinate communications with relevant stakeholders and the University community as necessary.
v) If necessary, appoint a delegate (liaison and communications officer) to manage communications with the CIO, Campus IT Leaders Group (ITLG) and University leadership throughout the incident response process. Notifications should be in written form to ensure there is an accurate record of events, unless otherwise directed.
vi) If necessary, designate a CSIRT member to act as liaison to the University's Emergency Operations Committee (EOC).
vii) Engage Treasury Operations and the University cyber security insurance provider when necessary as defined by this policy.
viii) Report incident to the University of Guelph Government Relations and Community Engagement team (gov.community@uoguelph.ca) as needed.
ix) In the event of a suspected privacy breach, coordinate with the University Secretariat to determine if notification to the Information and Privacy Commissioner of Ontario (IPC) is necessary.
x) Convene the CSIRT based on the recommendation from the Information Security team according to the Cyber Security Incident Response Process (Appendix A).
xi) Coordinate actions and communications with relevant stakeholders and the University community as necessary.

7) Chief Information Officer (CIO)

i) Receive notice of Major and Significant IT incidents from the CISO, Information Security team, or other sources (internal or external to the University) and share appropriately with stakeholders.
ii) Ensure University leadership is kept apprised of the incident, including members of the Emergency Operations Committee (EOC).
iii) Review and approve changes to this policy and associated process documentation.
iv) Ensure appropriate budget and resources are allocated to enable Information Security and the CSIRT to effectively respond to cyber security incidents.

Related Policies, Guidelines, and Processes

- University of Guelph Emergency Management Plan
- Acceptable Use Policy for Information Technology
- Records Management Policy
- Information Security Statement on Ransomware
- Data Storage Guidelines
- CCS Major Incident Communications Plan (available only to CCS Management Team)
- CCS Emergency Contact List (available only to CCS Management Team)

Definitions

Personally identifiable information (PII) - Personally identifiable information includes information about one's age, race, sex, marital status, educational and medical history, unique numbers such as Social Insurance Number (SIN) or student numbers, and one's name when used in conjunction with another identifying piece of information. Refer to the Freedom of Information and Protection of Privacy Act (FIPPA) for additional information.

Personal Health Information (PHI) – Personal health information is any identifying information about an individual in oral or recorded form that relates to the physical or mental health of that individual created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment. PHI is protected by the Ontario Personal Health Information Protection Act (PHIPA).

Information Security Event - An identified occurrence that is relevant to the confidentiality, integrity or availability of a system, service, or network state, indicating a possible breach of information security, a failure of controls, or that exposes security vulnerabilities.

Information Security Incident - A single or a series of unexpected or unwanted information security events that result in the successful realization of risk, causing damage, or the compromise of information security assets, systems, operations, or that threaten research.

Cyber Security Incident - Cyber security incidents are a subset of information security incidents primarily involving technology. Since most of our information and information systems are networked, cyber security incidents have the greatest likelihood of occurring and the greatest potential for damage.

Cyber Security Incident Response - The processes for detecting, reporting, assessing, responding to, dealing with, and learning from cybersecurity incidents. Also includes the actions taken to protect and restore a universities normal operational conditions of information systems, and the information stored in it, when a cybersecurity incident occurs.

Cyber Security Incident Response Team (CSIRT) - A team of appropriately skilled and trusted members of the University appointed to handle security incidents throughout their lifecycle.

Data Breach - A data breach is an incident in which sensitive, protected or confidential data has been accessed, stolen or altered by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), confidential information or intellectual property.

Denial of Service Attack - A denial of service (DoS) or distributed denial of service (DDoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. The most common kind of DoS attack is simply to send more traffic to a network address than it was designed to receive.

Service Level Disruption - An interruption or degradation of system/service availability or performance. Classification as a Major incident is dependent upon the duration, severity and impact of the disruption (e.g. performance degradation versus lack of availability), the criticality of the application/service, and the suspected source of the disruption (i.e. security related).

Vulnerability - A vulnerability is a weakness or gap in the University's protective efforts. This could include flaws in the design or configuration of software that has security implications.

Risk - Risk is the intersection of the likelihood and impact of a threat exploiting a vulnerability against University assets.

Malware - Malware is any malicious software intentionally designed to cause damage and/or enable unauthorized access to data, a computer, server or computer network.

Ransomware - Ransomware is a type of malware that prevents users from accessing their system or files until they pay a ransom to a malicious party, typically in the form of cryptocurrency.

University Leadership - Refers to the University's executive leadership including the Provost and the President.

Tabletop Exercise – A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario. (Source - NIST SP 800-84)

Appendix A: Cyber Security Incident Response Procedure

Introduction

Incident management includes detecting and responding to cyber security incidents and taking proactive steps to prevent incidents from occurring in the future. A formal Cyber Security Incident Response Team (CSIRT) has responsibility for managing and supporting rapid response to Major information security incidents. At the University of Guelph, the authority to form this CSIRT team and for responding to cyber security incidents is documented in the Cyber Security Incident Management Policy above.

Purpose

The rationale for chartering a Cyber Security Incident Response Team is to:

1. Create the capability to plan for Major information security incidents in advance,

2. specify a consistent predetermined course of action for investigations and incident resolution,

3. identify the individuals and units that need to be involved in investigating and resolving a Major information security incident,

4. facilitate rapid response to major disruptions of IT systems or services, and

5. develop consistent escalation and notification processes for managing major information security incident communication.

Goals

- Create a stable cadre of staff who understand both functional business processes and the general nature of the University's information technology infrastructure and enterprise systems.
- Develop familiarity with the fundamentals of incident handling processes.
- Develop standard protocols for classifying, prioritizing, escalating, responding to and containing security incidents.
- Consult with IT experts and appropriate University units with specific technical expertise as required.
- Refer incidents and/or findings to appropriate University processes consistent with relevant University policies.
- Analyze incidents after resolution to identify and remediate weaknesses in response processes, applications, and infrastructure.
- Conduct frequent tabletop exercises to identify weaknesses in the response process and to keep staff and management in a constant state of preparedness.

CSIRT Charter

The Chief Information Officer (CIO) is the formal sponsor of the Cyber Security Incident Response Team (CSIRT). The Chief Information Security Officer (CISO) will convene and oversee the CSIRT when active. If the CISO is not available, the CIO or an appointed delegate can also engage the CSIRT. The CISO will appoint each member of the CSIRT in conjunction with their applicable Unit Manager and manage the logistics of arranging immediate response to the in-scope incidents.

The CSIRT will be a stand-by team of individuals selected for their institutional knowledge of business processes and the University's technology infrastructure.

An important aspect of the CSIRT capability is proactive planning for adverse events. When a Major or Significant incident (disruption or attack) is in progress, decisions must be made quickly. The CSIRT has a mandate to develop standard protocols and capabilities for timely responses which are appropriate, efficient, and thorough. In support of this mandate, the CSIRT will conduct an annual review and test of these plans and procedures by conducting a tabletop exercise or similar activity.

CSIRT Activation

The CSIRT will normally be convened when a Major or Significant incident has been declared by the Information Security team, subject to the approval of the CISO. The applicable supervisors of each CSIRT member will be notified (concurrently with the members) when the CSIRT is convened. The Charter also provides for assembling the CSIRT in advance of an incident to conduct response planning and development of standard practices.

Major security incidents which trigger the recommended activation of the CSIRT cannot be fully anticipated or documented herein. CSIRT activation will normally be recommended based on a preliminary assessment of the incident's characteristics and operational impact, but may be triggered by any of the following:

- A **breach** (i.e. unauthorized exposure) of sensitive or confidential University data (including personally identifiable information), the source or cause of which is initially unknown or uncertain.
- A **malware** or **ransomware** infection affecting multiple systems or representing an impact to campus services.
- A serious and **on-going disruption** of an enterprise business system or central technology service/infrastructure, the cause of which is suspected to be security related.
- A multi-site (or multi-node) security event, affecting **multiple computers** or **many users**.
- **An intrusion in progress** with the potential to seriously damage or disrupt operations.
- A security-related threat, not currently active, but having **campus-wide scope** or involving **enterprise/critical systems** or infrastructure.
- Any security-related incident which involves **external media** (press), or a potential **breach of legislative compliance** (e.g. FIPPA).

All information security incidents will be categorized and tracked in the centrally managed ticketing system, and reports will be generated on a monthly basis by the Information Security team. These reports will be made available to the CIO and other parties approved by the CIO as necessary.

When activated, the CSIRT will utilize University supported collaboration tools, such as Microsoft Teams, to organize and mobilize. In the event that these tools are impacted by the incident, alternative solutions, such as phone bridges or in-person incident rooms, will be utilized. The intention of this document is not to be prescriptive with respect to the technology utilized,

however, the CSIRT team must be mindful of the sensitivity of the data being discussed and shared on these platforms.

CSIRT Responsibilities

The Cyber Security Incident Response Team is responsible for the following:

1. Record and document all reports of Major information security incidents.
2. Verify the existence and scope of reported incidents.
3. Make a preliminary assessment of the incident's impact and current status.
4. Engage additional resources from supporting teams as needed in a timely manner to investigate and recover services.
5. Follow the established CCS Major Incident Communications Plan.
6. Provide regular status updates to the CISO.
7. Establish and maintain communication with applicable Department Chairs or Managers of the affected units or systems.
8. Ensure that the Campus Safety Office have been advised when criminal activity is alleged.
9. Advise University Secretariat if a data breach involving confidential records or personal information is alleged.
10. Advise the Vice President Finance, Administration & Risk and Chief Internal Auditor in the event that there is a financial impact to the University, or the incident is related to financial systems.
11. Liaise with Campus Safety Office and external forensic consultants to gather evidence as required.
12. Hold a post-incident debrief session to review the incident to continuously improve response plans and prevent similar occurrences in the future.