Information Security Incident Reporting

[Revised SPG 601.25]

I. Purpose

It is the policy of the University of Michigan to handle information technology security incidents efficiently, consistently, and carefully so as to minimize their impact on the confidentiality, integrity, and availability of the university’s systems, applications, and data. An effective approach to managing such incidents also limits the negative consequences to both the university and individuals and improves the university’s ability to promptly restore operations affected by such incidents.

It is especially important that serious incidents that may result in disruptions to important business processes are promptly communicated to the appropriate university officials so that they are involved early in decision making and communications. In addition, compliance with various federal and state regulatory mandates requires expeditious reporting of certain types of incidents.

While information security incidents are not always preventable, appropriate procedures for incident detection, reporting and handling, combined with education and awareness of the U-M community, can minimize their frequency, severity, and potentially negative individual, operational, reputational, and financial consequences.

The goals of establishing a successful incident management capability include:

A. Mitigating the impact of IT security incidents.
B. Identifying the sources and underlying causes of IT security incidents and unauthorized disclosures to aid in reducing their future frequency of occurrence.
C. Protecting, preserving, and making usable all information regarding the incident or disclosure as necessary for forensic analysis and notification.
D. Ensuring that all parties are aware of their responsibilities regarding IT system security incident handling.
E. Protecting the reputation of the university.

II. Definitions

A. An information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or violation of explicit or
implied proper use policy (as defined in Proper Use of Information Resources, SPG 601.07). Examples of information security incidents include (but are not limited to):

- Computer security intrusion
- Unauthorized or inappropriate disclosure of sensitive institutional data
- Suspected or actual breaches, compromises, or other unauthorized access to U-M systems, data, applications, or accounts
- Unauthorized changes to computers or software
- Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive, personally owned device used for university work) used to store private or potentially sensitive information
- Denial of service attack or an attack that prevents or impairs the authorized use of networks, systems, or applications
- Interference with the intended use or inappropriate or improper usage of information technology resources.

While the above definition includes numerous types of incidents, the requirement for central security incident reporting, regardless of malicious or accidental origin, is limited to serious incidents as defined below.

Occurrences such as incidental access by employees or other trusted persons where no harm is likely to result are not considered information security incidents.

B. A serious incident is an incident that may pose a substantial threat to university resources, stakeholders, and/or services. Specifically, an incident is designated as serious if it meets one or more of the following criteria:

- Involves potential, accidental, or other unauthorized disclosure external to U-M of sensitive information (as defined below)
- Involves serious legal issues including criminal activity, or may result in litigation or regulatory investigation
- May cause severe disruption to mission critical services
- Involves active threats
- Is widespread
- Is likely to be of public interest

C. Sensitive information is defined in Institutional Data Resource Management Policy, (SPG 601.12) as information whose unauthorized disclosure may have serious adverse effect on the university’s reputation, resources, services, or individuals. Information protected under federal or state regulations or due to proprietary, ethical, or privacy considerations will typically be classified as sensitive. Sensitive information includes personally identifiable information such as protected health information (PHI), Social Security numbers, credit card numbers, and any other information designated as sensitive by the university Data Stewards.

D. The Information security coordinator is an individual staff or faculty member or a group that has been designated by the unit dean or director to provide unit oversight of
information security, communicate and coordinate related activities with Information and Infrastructure Assurance (IIA), evaluate and respond to non-serious incidents, and coordinate unit response to risk assessments and audit requests. Coordinators will develop and implement unit-level policies, procedures, communications, and educational awareness programs consistent with university-wide guidance. The information security coordinator may be the unit IT service provider, the unit security or compliance officer, or any other individual within or outside the given unit that is so designated.

III. Policy

A. All users of university IT resources must report all information security incidents, irrespective of level of severity, to their unit’s information security coordinator or IT service provider as soon as possible, but no later than 24 hours from the time the incident is identified.

B. Any event that appears to satisfy the definition of a serious IT incident must be reported to the appropriate authority listed below under Roles and Responsibilities as soon as possible, but no later than 24 hours from the time the incident is identified.

C. Some IT incidents may also be crimes (e.g. threats to personal safety or physical property or illegal activities) which should be immediately reported to the U-M Police Department concurrent with the incident notification described in this policy.

D. To avoid inadvertent violations of state or federal law, individuals and departments may not release information, electronic devices, or electronic media to any outside entity, including law enforcement organizations, before making the notifications required by this policy.

E. Privacy and Confidentiality of Sensitive Information:
   - When university staff report, track, and respond to information security incidents, they must protect and keep confidential any sensitive information.
   - Incident data retained for investigation will exclude any sensitive information that is not required for incident response, analysis, or by law, regulation, or university policy.

IV. Roles and Responsibilities

A. The University Chief Information Security Officer is the ultimate authority for interpretation and implementation of this SPG, as well as for coordinating incident communications. The Office of the University Chief Information Security Officer will retain relevant records and evidence pertaining to all serious incidents for a period of three years after the occurrence of the event. For incidents involving unauthorized disclosure of PHI, records will be retained for six years.

B. Information and Infrastructure Assurance (IIA) will oversee, coordinate, and guide the incident management process to promote a consistent, efficient, and effective response, including compliance with applicable breach notification laws and regulations. IIA staff serve as the information security coordinator for Information and Technology Services and all MiWorkspace units.
In addition, IIA may:

1. Convene, when appropriate, a multi-department Computer Security Incident Response Team (CSIRT).
2. Collaborate and coordinate with other university offices including applicable compliance offices as necessary.
3. Take steps to preserve forensic evidence through a documented and repeatable process.
4. Prepare a final report on the incident that summarizes findings and, if appropriate, makes recommendations for improvement designed to prevent recurrence of similar incidents.
5. Conduct ongoing education and awareness for the U-M community.

C. Users of University Information Technology Resources: all faculty, staff, and workforce members must promptly report all information security incidents—non-serious and serious—to their unit information security coordinator, or in the absence of a coordinator, directly to their unit IT service provider.

D. Information Security Coordinators:

a) Information security coordinators must promptly report suspected serious incidents (which are reported to or identified by them). When an incident involves the types of sensitive information below, the coordinators must promptly report the incident to the following parties:

- **If an incident involves protected health information (PHI),** information security coordinators must report the incident to Information and Infrastructure Assurance (IIA) at security@umich.edu and the University HIPAA Privacy Director at UMHS-Compliance-IT-Sec@med.umich.edu.
- **If an incident involves any human subject research information,** information security coordinators must report the incident to IIA at security@umich.edu and the Office of Research (UMOR) UMOR-IT-Sec@umich.edu.
- **If an incident involves both protected health and human subject research information,** information security coordinators must report the incident to IIA at security@umich.edu, the University HIPAA Privacy Director at UMHS-Compliance-IT-Sec@med.umich.edu, and the Office of Research (UMOR) at UMOR-IT-Sec@umich.edu.
- **If an incident involves payment card information (PCI),** a U-M merchant must report the incident to the Treasurer’s Office at merchantservices@umich.edu.

b) Information security coordinators will evaluate and respond to information security incidents in accordance with university and unit policies and procedures.

c) Information security coordinators will develop and implement unit-level policies, procedures, communications, and educational programs that are consistent with university-wide policies and procedures.

E. The University HIPAA Officer and UMOR will promptly inform IIA of serious incidents reported to them, except for those incidents that involve unethical or unacceptable behavior as described in SPG 601.07.
F. **Third-Party Vendors and Contractors:** U-M has a stewardship or custodial interest in all university data, regardless of how or where it is stored, transmitted, or processed. The reporting requirements of this policy apply to third parties that are contractually bound to limit the access, use, or disclosure of U-M information assets. These third-party vendors or entities shall promptly report potential or actual incidents to their primary U-M contact.

V. **Violations and Sanctions**

Violations of this policy may result in disciplinary action up to and including non-reappointment, discharge, dismissal, and/or legal action. Disciplinary action for faculty and staff shall be consistent with [Discipline (SPG 201.12)](https://example.com).

VI. **Reporting Incidents**

- Information and Technology Services (ITS) - [security@umich.edu](mailto:security@umich.edu)
- Incidents involving PHI: University HIPAA Officer - [UMHS-Compliance-IT-Sec@med.umich.edu](mailto:UMHS-Compliance-IT-Sec@med.umich.edu)
- Incidents involving human subject research: Office of Research - [UMOR-IT-Sec@umich.edu](mailto:UMOR-IT-Sec@umich.edu)

VII. **References**

[Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan (SPG 601.07)](https://example.com)
[Institutional Data Resource Management (SPG 601.12)](https://example.com)
[Information Security Policy (SPG 601.27)](https://example.com)