SPG U-M Standard Practice Guide

UNIVERSITY OF MICHIGAN

Standard Practice Guide Policies

Information Security Incident Reporting

601.25

Applies to: All Faculty and Staff

I. OVERVIEW

The University of Michigan actively manages information security incidents to minimize their impact on the confidentiality, integrity, and availability of the university's systems, applications, and data.

It is vital that suspected information security incidents are promptly reported to ITS Information Assurance (IA) in order to limit the negative consequences to the university and individuals, improve the university's ability to promptly restore operations affected by such incidents, and allow the university to meet regulatory reporting requirements.

IA engages appropriate stakeholders in the management of incident response, depending on incident scope and severity.

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 significant violation of the university policy on Responsible Use of Information Resources (SPG 601.07) (https://spg.umich.edu/policy/601.07). Examples of information security incidents include:

1. Computer system intrusion
2. Unauthorized or inappropriate disclosure of institutional data
3. Suspected or actual breaches, compromises, or other unauthorized access to U-M systems, data, applications, or accounts
4. Unauthorized changes to computers or software
5. 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 university data as defined in the policies on Institutional Data Stewardship (601.12) (https://spg.umich.edu/policy/601.12) and Research Data Stewardship (SPG 303.06) (https://spg.umich.edu/policy/303.06)
6. Denial of service attack or an attack that prevents or impairs the authorized use of networks, systems, or applications
7. Interference with the intended use or inappropriate or improper usage of information technology resources.

B. A **serious information security incident** poses a substantial threat to university resources, stakeholders, and/or services. An incident is designated as serious if there is a likelihood that it:

1. Involves computer system intrusion, breach, compromise, or other unauthorized access to U-M systems, data, applications, or accounts
2. Involves potential, accidental, or other unauthorized access or disclosure of "High" or "Restricted" institutional data
3. Involves legal issues including criminal activity, or may result in litigation or regulatory investigation
4. May cause severe disruption to mission critical services
5. Involves active threats
6. Is widespread
7. May be of public interest
8. May cause reputational harm to the university

III. SCOPE

This policy applies to the Ann Arbor campus, Michigan Medicine, UM-Dearborn, UM-Flint, and all affiliates. Specifically, the scope of this policy encompasses:

A. All faculty, staff, workforce members, and sponsored affiliates in all units;

B. Third-party vendors who collect, process, share or maintain university institutional data, whether managed or hosted internally or externally;

C. Personally owned devices of members of the U-M community that access or maintain sensitive institutional data.

IV. POLICY

A. All users of university IT resources must report all information security incidents to their IT security provider or security unit liaison.

B. Any event that appears to satisfy the definition of a serious information security incident must be reported to Information Assurance (IA).

C. It is expected that incident reporting, from identification to reporting to IA (if necessary), will occur within 24 hours.

D. Some information security incidents may also be criminal in nature (e.g., threats to personal safety or physical property) and in addition to IA, should be reported to the U-M Division of Public Safety and Security.

E. Some units may have regulatory or sponsor incident reporting requirements that are more restrictive. Units should inform IA of these requirements when reporting a security incident. IA will work with appropriate stakeholders to provide necessary reporting to regulatory or sponsoring agencies.

F. 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, without consulting with IA first.

V. ROLES AND RESPONSIBILITIES

A. **The University Chief Information Security Officer** is the ultimate authority for interpretation and implementation of this policy, as well as for coordinating serious information security incidents.

B. **ITS Information Assurance** (IA) determines the severity of information security incidents and oversees, coordinates, and guides the incident management process for serious information security incidents. IA ensures appropriate, consistent, efficient, and effective response, including compliance with applicable breach notification laws and regulations.

C. **Security Unit Liaisons** (https://safecomputing.umich.edu/it-security-professionals/security-unit-liaisons), designated by the unit dean or director to serve as the unit's IT security contact, evaluate and respond to non-serious incidents, and coordinate unit response to risk assessments and audit requests. Liaisons also develop and implement unit-level policies, procedures, communications, and educational awareness programs consistent with university-wide guidance. **Security Unit Liaisons or their designees** must report suspected serious incidents (reported to or identified by them) within the 24 hour timeframe.

D. **Users of University Information Technology Resources**, which include all faculty, staff, and workforce members, must report any suspected security events to security@umich.edu (mailto:security@umich.edu).

VI. VIOLATIONS AND SANCTIONS

Violations of this policy may result in disciplinary action up to and including suspension or revocation of computer accounts and access to networks, non-reappointment, discharge, dismissal, and/or legal action. Discipline (SPG 201.12) (/policy/201.12) provides for staff member disciplinary procedures and sanctions. Violations of this policy by faculty may result in appropriate sanction or disciplinary action consistent with applicable university procedures. If dismissal or demotion of qualified faculty is proposed, the matter will be addressed in accordance with the procedures set forth in Regents Bylaw 5.09. In addition to U-M disciplinary actions, individuals may be personally subject to criminal or civil prosecution and sanctions if they engage in unlawful behavior related to applicable federal and state laws.

VII. RELATED POLICIES

A. Responsible Use of Information Resources (SPG 601.07) (/policy/601.07)

B. Institutional Data Stewardship (SPG 601.12) (/policy/601.12)

C. Information Security (SPG 601.27) (/policy/601.27)

D. Report an IT Security Incident, Safe Computing (http://safecomputing.umich.edu/report-it-security-incident?nav)

Notes

August 2025: Updated to make policy clearer and more concise, clarify security incident vs. serious security incident, and removal of reporting guidelines from plicy to guidance available on website.

SPG Number:	**Applies To:**
601.25	All Faculty and Staff
Date Issued:	**Owner:**
July 10, 2006	Office of the Vice President for Information Technology and Chief Information Officer
Last Updated:	
August 22, 2025	**Primary Contact:**
Next Review Date:	Office of the Vice President for Information Technology and Chief Information Officer
August 22, 2030	

Related Policies:

Information Security (/policy/601.27)
Institutional Data Stewardship Policy (/policy/601.12)
Responsible Use of Information Resources (/policy/601.07)

Related Links:

Report an IT Security Incident, Safe Computing (http://safecomputing.umich.edu/report-it-security-incident?nav=)
General Information Technology Policies (https://it.umich.edu/information-technology-policies/general-policies)