THE UNIVERSITY OF MICHIGAN
STANDARD PRACTICE GUIDE

SECTION:	General University Policies and Procedures	**Number:**	601.25
		Revised:	
SUBJECT:	Information Security Incident Reporting Policy	**Date Issued:**	7/10/06
		Review Date:	7/10/10
APPLIES TO:	All Faculty and Staff	**Attachment(s)**	0
ISSUED BY:	Executive Vice President and Chief Financial Officer, Provost and Executive Vice President for Academic Affairs, and Executive Vice President for Medical Affairs		

I. Purpose

This policy serves to minimize the negative consequences of information security incidents and to improve the University's ability to promptly restore operations affected by such incidents. It ensures incidents are promptly reported to the appropriate University officials, that they are consistently and expertly responded to, and that *serious incidents*[1] are properly monitored.

II. Policy

A) Users of University Information Resources:
   a. Users of University information technology resources must promptly report all *information security incidents* to their unit *information security coordinator*.

B) *Information Security Coordinators*:
   a. Except as noted below, *Information security coordinators* must promptly report all *serious incidents* (which are reported to them or identified by them) to the Information Technology Security Services (ITSS).

      i. <u>If an incident involves any protected health information</u> (PHI), *information security coordinators* must report the incident to the University HIPAA Officer.

      ii. <u>If an incident involves any human subject research information</u> and has not already been reported to the University HIPAA Officer, *information security coordinators* must report the incident to the Office of the Vice President for Research (OVPR).

   b. The University HIPAA Officer and OVPR will inform ITSS of *serious incidents* reported to them, except for those incidents that involve unethical or unacceptable behavior as described in SPG 601.7.

   c. Incidents must be reported by users or by *information security coordinators* as soon as possible, but no later than within 24 hours from the time an incident is identified or initially reported.

   d. *Information security coordinators* will evaluate and respond to information security incidents in accordance with University and unit policies and procedures, including the Information Security Incident Management Guidelines[2].

[1] Words that appear in *italics* are defined in Section III, Definitions.
[2] See section V, References.

e. *Information security coordinators* will develop and implement unit-level policies, procedures, communications, and education programs that are consistent with University-wide policies and procedures.

C) Privacy and Confidentiality of Sensitive Information:

a. When University staff report, track, and respond to information security incidents, they must protect and keep confidential any *sensitive information*.

b. Tracked incident data will exclude any *sensitive information* that is not required for incident response, analysis, or by law, regulation, or University policy.

III. Definitions

a) An *information security incident* is defined as an attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy (as defined in SPG 601.7). Examples of information security incidents include (but are not limited to):

1. Computer security intrusion
2. Unauthorized use of systems or data
3. Unauthorized change to computer or software
4. Loss or theft of equipment used to store private or potentially sensitive information
5. Denial of service attack
6. Interference with the intended use of information technology resource
7. Compromised user account

While this definition covers numerous potential and actual incidents, the requirement for central incident reporting is aimed at *serious incidents* as defined below.

b) A *serious incident* is an incident that may pose a 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:

1. Involves potential unauthorized disclosure of *sensitive information* (as defined below)
2. Involves serious legal issues
3. May cause severe disruption to critical services
4. Involves active threats
5. Is widespread
6. Is likely to raise public interest

c) *Sensitive information* is defined in SPG 601.12 as information that "because of legal, ethical, or other externally-imposed constraints, may not be accessed without specific authorization or to which only limited access may be granted". In the context of the definition of a *serious incident, sensitive information* is defined as non-public information, as defined by law or practice, whose disclosure may have serious adverse effect on individuals and/or on the University. *Sensitive information* includes personally identifiable information such as protected health information (PHI), social security number, credit card numbers, and any other information designated as sensitive by the University Data Stewards.

d) *Information security coordinator* is a University department, a departmental unit or an individual staff person or faculty member that has been designated by the unit dean or director to act as the

unit information security coordinator. The *information security coordinator* may be the unit information technology service provider, the unit security officer, or any other individual or department within or outside a given University unit that is so designated by the unit.

IV. Contacts

- Information Technology Security Services (ITSS) - security@umich.edu
- University HIPAA Officer - UMHS-Compliance-IT-Sec@med.umich.edu
- Office of the Vice President for Research – OVPR.JLG@umich.edu
- Unit *information security coordinators* - as indicated in unit-specific sites. A list will also be posted at http://safecomputing.umich.edu/

Notes:
a) If the unit *information security coordinator* is not known, reporting to ITSS is required.
b) The University HIPAA Officer is the designated *information security coordinator* and security officer for the Health System.

V. References

Information Security Incident Management Guidelines
https://www.itss.umich.edu/umonly/im_guidelines.pdf
SPG 601.7 – Proper Use of Information Resources
http://spg.umich.edu/pdf/601.07-0.pdf
SPG 601.12 – Institutional Data Resource Management
http://spg.umich.edu/pdf/601.12.pdf