Information Security Policy

601.27

Applies to: All Faculty and Staff

Search this page

I. PURPOSE

This policy establishes University-wide strategies and responsibilities for protecting the *confidentiality*[1], *integrity*, and *availability* of the *information assets* that are accessed, managed, and/or controlled by the University. *Information assets* addressed by the policy include data, information systems, computers, network devices, as well as documents and verbally[2] communicated information.

By implementing this policy, the University will:

- Establish a University-wide information security framework to appropriately secure access to information resources and services;
- Protect against unauthorized access to, use, or sharing of, *sensitive information* that could potentially result in harm to the University or to members of the University community;
- Protect against anticipated threats or hazards to the security of information assets;
- Comply with federal, state, and local law, University policies, and agreements binding the University that require the University to implement applicable *security safeguards*.

II. POLICY

Additional information that supports this policy can be found in the Information Security Policy Supplement.

a. Members of the University community have individual and shared responsibilities to protect the information assets controlled by the University in accordance with federal, state, and local law, University policies, and agreements binding the University.

b. Each University *unit* will develop, maintain, and implement an information security plan. The plan will identify applicable regulations and will define unit security initiatives.

c. Each University *unit* will identify and track sensitive and critical Information assets under its control. *Information assets* will be classified relative to the level of risk that their compromise may pose to the institution. *Information asset* classification standards and guidelines will be adhered to.

d. Each University *unit* will periodically conduct risk assessments around its sensitive and critical *information assets*. Risk assessments will prioritize risks and recommend appropriate mitigation strategies.

e. Each University *unit* will report and manage information security incidents in accordance with established policies and guidelines, including SPG 601.25, Information Security Incident Reporting.

f. Each University *unit* will implement Security safeguards that are appropriate to *information asset sensitivity*, *criticality*, and the level of risk identified in the risk assessment process.

III. RESPONSIBILITIES FOR IMPLEMENTATION

University Deans and Directors are responsible for implementing and ensuring compliance with this policy. Responsibilities include:

The Chief Information Technology Security Officer is responsible for:

a. Communicating this policy to their community and ensuring appropriate education and training;

b. Designating individuals to unit information security roles, ensuring they are properly trained, and ensuring their ongoing participation in University-wide security activities;

c. Ensuring the implementation of information security plans within their units;

d. Ensuring unit collaboration on the implementation of the University-wide IT Security Program.

e. Directing and coordinating the University-wide IT Security Program;

f. Determining unit-level compliance with this policy;

g. Providing a focal point for oversight of serious security incidents as indicated in SPG 601.25, Information Security Incident Reporting;

h. Establishing security metrics, tracking the progress of the IT Security Program, and providing a University-wide risk profile;

i. Assisting units in fulfilling their information security requirements.

IV. DEFINITIONS

AVAILABILITY refers to the level of assurance that authorized users have access to information resources when required.

CONFIDENTIALITY refers to the level of assurance that information is not made available or disclosed to unauthorized individuals, entities, or processes.

CRITICALITY refers to the relative importance of the information to the mission of the University, and reflects the degree to which the information requires protection to ensure it is not accidentally or maliciously altered or destroyed.

INFORMATION ASSET refers to data, system, computer, network device, document, or any other component of the university infrastructure which stores, processes or transmits data.

INTEGRITY refers to the assurance that information is not accidentally or maliciously altered or destroyed.

SECURITY SAFEGUARDS refer to protective measures prescribed to meet security requirements (i.e., confidentiality, integrity, availability) specified for an information asset or environment. Also called security controls or countermeasures.

SENSITIVE INFORMATION refers to 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.

SENSITIVITY refers to the degree to which information requires protection to ensure it is not exposed to unauthorized users.

UNIT refers to any organization across the University such as a school, college, department, or central office. The Health System as well as the Flint and Dearborn campuses are considered University units.

V. REFERENCES

Data Steward/Data Manager List (http://cio.umich.edu/data-stewardship/data-management.php)

UMHS HIPAA Information (http://www.med.umich.edu/u/hipaa/index.htm)

U-M GLBA Information Security Program (https://www.safecomputing.umich.edu/sites/default/files/UM-GLBA-Information-Security-Program.pdf)

University Statement on Stewardship (https://hr.umich.edu/about-uhr/statement-stewardship)

Attachment	Size
University Student Rights and Records Policy (http://ro.umich.edu/ferpa/)	

[1] Words that appear in italics are defined in the Definitions section.

[2] HIPAA http://www.med.umich.edu/u/hipaa/index.htm requires taking reasonable precautions when verbally communicating protected health information. Precautions should also be taken when verbally communicating other *sensitive information*.

Attachment	Size
Printable PDF of SPG 601.27, Information Security Policy	186.81 KB

SPG number:
601.27

Date issued:
January 2, 2008

Next review date:
January 2, 2012

Applies to:
All Faculty and Staff

Owner:
Office of the Executive Vice President and Chief Financial Officer, the Office of the Provost and Executive Vice President for Academic Affairs, and the Office of the Executive Vice President for Medical Affairs

Primary contact:
Office of the CIO

Related policies:
Identity Misrepresentation
Information Security Incident Reporting
Institutional Data Resource Management Policy
Responsible Use of Information Resources

Related links:
ITS - Administrative Data Policies
U-M Health - Protecting your Privacy (HIPAA)
U-M Student Rights and Student Records
Information Technology Policies and Standards
U-M GLBA Information Security Program
Information Security Laws and Regulations
Social Security Number Privacy and Protection
Statement on Stewardship