SPG U-M Standard Practice Guide

UNIVERSITY OF MICHIGAN

Standard Practice Guide Policies

Information Security

601.27

Applies to: All Faculty, Staff, and Affiliates

1. Overview and Guiding Principles

The University of Michigan has legal, contractual, and ethical obligations to protect the confidentiality, integrity, and availability of its systems and data. This policy strikes a balance between protecting university systems and data, maintaining the open environment that enables faculty, staff, and students to excel, innovate, and collaborate across the world, and ensuring that U-M core missions and institutional priorities remain paramount. The university promotes and supports an institutional culture that elevates its overall information security posture by following these principles: :

- **One Information Assurance Program**. The university will establish and maintain a comprehensive, institution-wide information assurance and cybersecurity risk management framework and program.
- **Protection of Data and Information Assets**. The university will optimize its ability to protect institutional data, systems, resources, and services from unauthorized access and other threats or attacks that could potentially result in harm to the university or to members of the university community.
- **Shared Responsibility**. Members of the university community have individual and shared responsibilities to protect the university's information assets and comply with applicable laws, regulations, and policies.
- **Regulatory Compliance**. U-M will comply with federal, state, and local law, university policies, and contracts and agreements that require the university to implement security safeguards in as cost-effective manner as possible.
- **Secure U-M IT Services**. U-M will seek to maximize the use of secure and compliant university-provided services that are readily and affordably accessible to faculty, researchers, clinicians, and staff.

- **Education and Awareness**. The university and units have an obligation to educate, inform, and enable U-M community members to use information in a secure and compliant manner. Pr.

2. Scope

This policy is platform and technology neutral. It applies to the the Ann Arbor campus, Michigan Medicine, UM-Dearborn, UM-Flint, all affiliates, and all faculty, staff, workforce members, sponsored affiliates. It also encompasses:

- All institutional data, including administrative, teaching and learning, clinical, and research. Institutional data is defined as any data that is owned, licensed by, or under the direct control of the university, whether stored locally or with a cloud provider.
- Third-party vendors who collect, process, share, or maintain university institutional data, whether managed or hosted internally or externally.
- Personally owned devices of members of the U-M community that access or maintain sensitive institutional data classified as **Restricted** or **High**.

3. Policy

All institutional data must be protected in accordance with the provisions below, which take into consideration the level of sensitivity and criticality that the data has to U-M.

- **Sensitive Data Classification**: All university information is classified into one of four levels based on its sensitivity and risk of harm to individuals and the university if the information is subject to a breach or unauthorized disclosure. Harm may encompass negative psychological, reputational, financial, personal safety, legal, or other ramifications to individuals or the university, or otherwise result in an adverse impact on the university's mission, research activity, or operations.
- **Data Security**: The university establishes minimum security controls appropriate for safeguarding data based on the data's classification level.
- **Risk Management**: The university maintains a risk-management framework which requires periodic risk assessments of systems and applications that maintain sensitive institutional data.
- **Risk Acceptance:** U-M executive officers exercise authority to accept information security and privacy related risks to the university's information assets. U-M units and individuals may not unilaterally accept information security, privacy, and compliance risks that have the potential to increase the university's vulnerability to cyber risks.
- **Privacy Review**: The U-M Privacy Officer will coordinate any review of the privacy or civil liberties implications and risks of the university's information assurance program, and its information security technologies or activities to minimize or mitigate such risks.

4. Supplemental IT Standards

This information security policy is supported and supplemented by specific operational, procedural, and technical standards. These Standards are mandatory and are enforced in the same manner as this policy.

This policy recognizes the need to accommodate unique research, teaching, and clinical needs that may not be practicable to accomplish through the use of U-M IT services provided by the major institutional IT providers. In those cases, it is the the responsibility of the unit or user to adhere to the appropriate information security requirements as outlined in this policy and the supplemental Standards.

5. Oversight and Enforcement

The Office of the Chief Information Security Officer (CISO) is responsible for the development, implementation, monitoring, and enforcement of the university's information security program. Other university staff perform essential information security and cybersecurity risk management functions contributing to program implementation and regulatory compliance.

The CISO will periodically present an update on the status of the university information assurance program to U-M IT governance bodies, executive officers, and the Board of Regents.

6. 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. In addition, the connectivity of machines and servers to the U-M network that do not comply with this policy or its associated Standards may be limited or removed.

Any U-M department or unit found to have violated this policy may be held accountable for the financial penalties, legal fees, and other remediation costs associated with a resulting information security incident and other regulatory non-compliance.

7. Related Policies

- Information Security Incident Reporting (SPG 601.25) (http://spg.umich.edu/policy/601.25)
- Institutional Data Resource Management Policy (SPG 601.12) (http://spg.umich.edu/policy/601.12)
- Responsible Use of Information Resources (SPG 601.07) (http://spg.umich.edu/policy/601.07)
- Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data (SPG 601.33) (http://spg.umich.edu/policy/601.33)
- Statement on Stewardship: Stewardship of Information and Technology Resources (https://hr.umich.edu/about-uhr/statement-stewardship)

File Attachments

Printable PDF of SPG 601.27, Information Security (http://www.spg.umich.edu/sites/default/files/policies/601x27_0.pdf)

SPG Number:
601.27

Date Issued:
January 2, 2008

Last Updated:
June 20, 2018

Next Review Date:
June 20, 2023

Applies To:
All Faculty, Staff, and Affiliates

Owner:
Office of the Vice President for Information Technology and Chief Information Officer

Primary Contact:
Information Assurance

Related Policies:
Information Security Incident Reporting (/policy/601.25)
Institutional Data Resource Management Policy (/policy/601.12)
Responsible Use of Information Resources (/policy/601.07)
Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data (/policy/601.33)

Related Links:
Statement on Stewardship: Stewardship of Information and Technology Resources (https://hr.umich.edu/about-uhr/statement-stewardship)

Hard copies of this document are considered uncontrolled. If you have a printed version, please refer to the University SPG website (spg.umich.edu) for the official, most recent version.