Information Security and Assurance
(SPG 601.27)

Overview and Purpose
The University of Michigan, like other global research institutions, is a target for ever-escalating cybersecurity, privacy, and compliance risks and threats. As the steward of a very large volume of sensitive information and intellectual property, the university 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 and maintaining the open environment that enables faculty, staff, and students to excel, innovate, and collaborate across the world.

By implementing this policy, the university will:

● Establish and maintain a single, comprehensive institution-wide information assurance and cybersecurity risk management framework and program, based on an enterprise security architecture that makes leveraging secure services straightforward, and accessible to faculty and staff;
● Protect institutional data, systems, resources and services against unauthorized access and other anticipated threats or attacks that could potentially result in financial, legal, or reputational harm to the university or to members of the university community;
● Comply with federal, state, and local law, university policies, and contracts and agreements that require the university to implement applicable security safeguards;
● Ensure U-M core missions and institutional priorities remain paramount while protecting university information assets.

Guiding Principles
The university promotes and supports an institutional culture that elevates its overall information security posture by following the following principles:

● One Information Assurance Program: The university will adopt a unified and consistent approach to information assurance. It will incorporate security, privacy, and disaster recovery throughout the lifecycle of its enterprise architecture, system and application development, and IT hardware and software procurement. To the extent practicable, units and individual faculty, researchers, and staff will be expected to use common tools, information systems, processes, and services.
● 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.
- **Risk Management and Acceptance**: The university will establish, implement, and maintain a risk management framework that is approved and endorsed by campus IT governance. In general, U-M units and individuals should not unilaterally accept information security and compliance risk that results in the greater university’s vulnerability to cyber risks.
- **Standards-based**: U-M strives to align to the federal NIST Cybersecurity Framework Core and the security and risk management standards of NIST 800-53.
- **Privacy**: Privacy is fundamental to the university’s mission, value, and culture. The U-M Privacy Officer will collaboratively develop and maintain privacy principles, policies, standards, guidelines, and practices that meet legal and compliance requirements, and that support the university's mission.
- **Monitoring**: The university will monitor on an ongoing basis the security technologies and controls that support this policy to determine their effectiveness, compliance with statutory and regulatory requirements, and changes to the university’s information systems and technology environment.

**Scope**

This policy is platform and technology neutral, and applies to the entire university, including the Ann Arbor campus, Health System, U-M Dearborn, U-M Flint, Athletics, and all affiliates. Specifically, the scope of this policy encompasses:

- Faculty, staff, and all units;
- All institutional data, including administrative, teaching and learning, clinical, and research;
- 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.

**Policy**

- **Data Classification**: All university information is classified into one of four levels, identified in the table below, 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 mission or operations of the university. Classification of data should be performed by the appropriate University Data Steward.

<table>
<thead>
<tr>
<th>Data Classification by Sensitivity Level</th>
<th>Definition</th>
<th>Risk Level of Disclosure or Unauthorized Access</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Encompasses public</td>
<td>Not likely to cause harm or</td>
<td>Directory information;</td>
</tr>
<tr>
<td>Classification</td>
<td>Description</td>
<td>Moderate Impact</td>
<td>Examples</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Information</td>
<td>and data that anyone regardless of institutional affiliation can access</td>
<td>have an adverse impact on individuals or the university</td>
<td>information in public domain; public websites; institutional and business</td>
</tr>
<tr>
<td></td>
<td>without limitation.</td>
<td></td>
<td>information/data not identified as confidential or otherwise restricted</td>
</tr>
<tr>
<td>Moderate</td>
<td>Encompasses information and data that is individually identifiable; includes</td>
<td>Moderate harm to individuals or the university</td>
<td>Student Records/FERPA; human subject research; IT security information;</td>
</tr>
<tr>
<td></td>
<td>confidential or proprietary institutional records; or subject to contractual</td>
<td></td>
<td>donor records</td>
</tr>
<tr>
<td></td>
<td>agreements or regulatory compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>Encompasses information and data that is both individually identifiable and</td>
<td>Significant harm to individuals or the university; could expose the university</td>
<td>Personal Health Information/HIPAA; Social Security Numbers; sensitive</td>
</tr>
<tr>
<td></td>
<td>highly sensitive or confidential and usually subject to regulatory compliance</td>
<td>to criminal and civil liability</td>
<td>identifiable human subject research</td>
</tr>
<tr>
<td>Restricted</td>
<td>Encompasses information and data that are covered by specific prescriptive</td>
<td>Severe harm to individuals and the university; could expose the university to</td>
<td>Credit card information/PCI; FISMA; Export Controls/ITAR, EAR</td>
</tr>
<tr>
<td></td>
<td>information security controls and the most stringent legal or regulatory</td>
<td>criminal and civil liability</td>
<td></td>
</tr>
<tr>
<td></td>
<td>requirements</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Use of Approved IT Services:** Data is required to be stored in approved IT services or secured following specific and level-appropriate information security requirements based on the above classifications. The highest level of security controls should be applied to Restricted data.
  - The primary means of reducing and mitigating cyber risks is for units and individual faculty, researchers, and staff to use the university’s secure facilities and common information technology infrastructure and services whenever feasible.
- **Adherence to IT Security Standards and Requirements:** This policy recognizes the need to accommodate unique research, teaching, and clinical needs that may not be practicable to accomplish through the use of common IT services. In those cases, it is the unit or user responsibility to adhere to the appropriate information security requirements as outlined in this policy and associated Standards.
- **Certification of Unit-based System Security:** Units that maintain independent systems that maintain Moderate, High, or Restricted risk information must annually certify that they are maintaining the appropriate information security requirements.
- **Privacy Review:** The U-M Privacy Officer will coordinate any review of the privacy or civil liberties risks of the university’s information security functions and information assurance program to minimize or mitigate such risks.
Incident Reporting: Units will report and manage information security incidents in accordance with Information Security Incident Reporting (SPG 601.25).

Education and Awareness: The university will implement and maintain on an ongoing basis an information security best practices education, awareness, and training program directed at students, faculty, and staff.

Supplemental IT Standards
This information security policy is supported and supplemented by specific operational, procedural, and technical standards and requirements which are required to be compliant with applicable university policies, laws and regulations. These Standards will be periodically updated to meet emerging threats, changes in legal and regulatory requirements, and technological advances.

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 roles and responsibilities related to information security and cyber security risk management are described in Information Security Roles and Responsibilities.

The Office of the CISO will evaluate exception requests to this policy on a case-by-case basis, accounting for level of risk, potential threats and vulnerabilities, cost analysis, available staff resources, and operational and technical limitations or constraints.

The CISO will present an update on the status of the university IT security program to the appropriate Regental committee, executive officers, IT Executive Committee, and the IT Council on at least an annual basis.

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 disconnected.

Discipline (SPG 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.
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.

Third party vendors found to have violated this policy may incur financial liabilities in addition to contract termination.
Related Policies:

- Information Security Incident Reporting Policy (SPG 601.25)
- Institutional Data Resource Management Policy (SPG 601.12)
- Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan (SPG 601.07)
- Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data (SPG 601.33)
- Statement on Stewardship: Stewardship of Information and Technology Resources

Resources

- [SPG 601.27 Revisions and Recommendations](https://example.com) Google Doc