Information Assurance and IT Security
(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 wide variety 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 utilizing secure university-provided services straightforward and readily accessible to faculty and staff;

● Protect institutional data, systems, resources and services against unauthorized access and other 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 ensuring the confidentiality, integrity, authentication, and availability of university information assets, and reducing and better managing cybersecurity risks.

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 best practices throughout the lifecycle of its enterprise architecture, system and application development, research projects, clinical applications, and IT hardware and software. To the extent practicable, units and individual faculty, researchers, and staff will use common tools, information systems, processes, and services. The university recognizes, however, that it is organizationally and functionally very complex, and that campus units, research programs, and clinical care settings will have unique risks – different threats, different vulnerabilities, different risk tolerances. Consequently,
variations in how this policy and its supplemental IT Standards are implemented will be managed and tracked through an exceptions process.

- **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. Specifically, compliance by students, faculty, and staff with the recommended actions and behaviors included in Responsible Use of Information Resources (SPG 601.07) is an important contribution to the overall security of the U-M computing environment.

- **Risk Management and Acceptance**: The university will establish, implement, and maintain a risk management framework that is approved and monitored by campus IT governance. The university and individual units and research projects are required to conduct periodic risk assessments of systems and applications that maintain sensitive institutional data. These assessments help in the identification and prioritization of risk to critical infrastructure and services, allowing campus IT governance and leadership to make informed decisions regarding resource allocation and expenditures needed to reduce information security risks to an acceptable level. In general, U-M units and individuals may not unilaterally accept information security and compliance risks that have the potential to increase 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**: Respecting the privacy of its community members is fundamental to the university’s mission, value, and culture. The university will balance its cybersecurity obligations and activities while protecting individual privacy and civil liberties. The U-M Privacy Officer will collaboratively develop and maintain privacy principles, policies, standards, guidelines, and practices that meet legal and compliance requirements and transparency expectations, while supporting the university’s mission.

- **Program Effectiveness**: 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 university’s mission or operations. U-M data stewards are primarily responsible to determine classification of data.

<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 (non-sensitive)</td>
<td>Encompasses public information and data that anyone regardless of institutional affiliation can access without limitation.</td>
<td>Disclosure to the general public poses little or no risk to the University’s reputation, resources, services, or individuals.</td>
<td>Directory information; information in public domain; public websites; institutional and business information/data not identified as moderate or higher</td>
</tr>
<tr>
<td>Moderate (sensitive)</td>
<td>Encompasses information and data that is individually identifiable; includes confidential or proprietary institutional records; or subject to contractual agreements or regulatory compliance</td>
<td>Moderate harm to individuals or the university</td>
<td>Student Records/FERPA; human subject research; donor records</td>
</tr>
<tr>
<td>High (sensitive)</td>
<td>Encompasses information and data that is both individually identifiable and highly sensitive or confidential and usually subject to regulatory compliance</td>
<td>Significant harm to individuals or the university; could expose the university to criminal and civil liability</td>
<td>Identifiable health/medical Information/HIPAA; Social Security Numbers; sensitive identifiable human subject research; IT security information</td>
</tr>
<tr>
<td>Restricted (sensitive)</td>
<td>Encompasses information and data that are covered by specific prescriptive information security controls and the most stringent legal or regulatory requirements</td>
<td>Severe harm to individuals and the university; could expose the university to criminal and civil liability</td>
<td>Credit card information/PCI; FISMA; Export Controls/ITAR, EAR</td>
</tr>
</tbody>
</table>

- **Use of Approved IT Services**: The primary means of reducing and mitigating IT security and compliance risks is for units and individual faculty, researchers, and staff to use the university’s secure common information technology infrastructure, services, and facilities whenever feasible. Accordingly, this policy requires that data be stored in approved IT services or secured following specific and level-appropriate information security requirements based on the above classifications.
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 the supplemental IT Standards described below.

Certification of Unit-Based System Security: Units that maintain independent IT systems or applications that manage or store High or Restricted information must annually certify that they are maintaining appropriate information security requirements as provided for in this policy and the supplemental IT Standards, or have an approved exception.

Privacy Review: The U-M Privacy Officer will coordinate any review the privacy or civil liberties implications and risks of the university’s information security technologies or activities, 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 (see Appendix A for list). These Standards are required and are enforced in the same manner as this policy. They will be periodically reviewed and updated as necessary 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.

Compliance with this policy may be subject to review by University Audits, Office of Research Ethics and Compliance, Health System Compliance, or other institutional compliance areas.

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 annually 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.
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