Information Security
MICHIGAN STATE UNIVERSITY

DRAFT MSU Information Security Standards

Purpose:

To minimize risk to the University by providing information security standards that build upon the MSU Information Security policy to protect University systems, resources, and data.

Scope:

These standards apply to any University systems, resources, or data, and any persons or accounts that access any University systems or resources, or store, process, or transmit any University data.

Table of Contents

Standards Details:

I. General

1. Any persons or resources subject to these standards must comply with all applicable laws, regulations, and policies.

II. Access Control

Purpose: To minimize risk to the University resulting from unauthorized access to resources and help preserve and protect the confidentiality, integrity, and availability of University networks, systems, applications, and data.

III. Audit and Accountability

Purpose: To minimize risk to the University by providing the ability to detect malicious or anomalous activity, and to allow for the forensic reconstruction of events.

1. All University systems must audit events to a level sufficient to allow visibility into malicious campaigns within the MSU technology environment.

IV. Awareness and Training

Purpose: To minimize risk to the University by raising awareness of security and security related issues, and by providing training on topics including: individual responsibilities, acting in a secure fashion when using University resources, and what to do when a security related incident occurs.

V. Configuration Management

Purpose: To minimize risks to the University systems by ensuring all systems have basic security controls and are configured properly to support their designated function, and changes to those systems are properly analyzed, documented, and approved prior to implementation.

VI. Contingency Planning

Purpose: To minimize risk to the University by ensuring plans and procedures are in place which will allow for the continuation of University services should a catastrophic event or disaster occur.

VII. Identification and Authentication

Purpose: To minimize risk to the University by ensuring University resources can only be accessed by authorized individuals and services.

VIII. Incident Response

Purpose: To minimize risk to the University by ensuring plans, procedures, and training are in place that support the timely analysis, reporting, and resolution of security incidents.

IX. Maintenance

Purpose: To minimize risk to the University by establishing proper maintenance processes that reduce the likelihood of hardware and software failures.

X. Media Protection

Purpose: To minimize risk to the University by protecting digital and non-digital media, limiting access to the information on media to authorized users, and providing processes to sanitize or destroy media before its disposal or release for reuse.

XI. Personnel Security

Purpose: To minimize risk to the University by providing processes to screen personnel for potential security risks, and by ensuring that University resources are protected during and after personnel actions, such as terminations and transfers.

XII. Physical and Environmental Protection

Purpose: To minimize risks to the University by limiting physical access to University resources to authorized individuals, protecting physical infrastructure, and providing appropriate environmental controls in facilities containing University systems.

XIII. Planning

Purpose: To minimize risk to the University by ensuring a security plan is in place that describes the security controls to be used, as well as the rules of behavior for individuals accessing University systems.

XIV. Program Management

Purpose: To minimize risk to the University by establishing an information security program that is designed to reduce risk to an acceptable level, coordinates with and is supportive of the University's mission and business needs.

XV. Risk Assessment

Purpose: To minimize risk to the University by providing the means to periodically assess the risk to University operations and University resources.

XVI. Security Assessment and Authorization

Purpose: To minimize risk to the University by providing a means to monitor and assess security controls to ensure their continued effectiveness.

XVII. System and Communications Protection

Purpose: To minimize risk to the University by ensuring that University communications are monitored, controlled, and protected at external boundaries and key internal boundaries.

1. Before being exposed to the internet, all University systems must comply with all applicable requirements within this standard, as determined by MSU Information Security.
2. Any University system that is configured to allow remote administration must utilize either key-based authentication or multi-factor authentication.
3. Any University system that is configured to use FTP/S must:
   3.1. Configure ephemeral PASV ports to the range of TCP 60000-60100.
   3.2. Have a valid security certificate installed that meets the minimum configuration standards set forth by MSU Information Security.

XVIII. System and Information Integrity

Purpose: To minimize risk to the University by providing protection from malicious code, monitoring security alerts and advisories, and ensuring that system flaws are identified, reported, and corrected in a timely manner.

1. All University systems must be enrolled in a vulnerability management program that identifies all critical security vulnerabilities.
   1.1. All identified critical security vulnerabilities must be patched or fixed within one month of identification of the vulnerability, or availability of the patch or fix, whichever is later.
2. All University systems must be enrolled in a patch management program that is designed to apply all security patches produced by the vendor or manufacturer within one month of release.
3. All University systems must be protected against the installation of malware.

XIX. System and Services Acquisition

Purpose: To minimize risk to the University by allocating sufficient resources to adequately protect University systems, employing software development life cycle processes that incorporate information security considerations, employing software usage and installation restrictions, and ensuring that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the University.

Roles and Responsibilities:

- All MSU faculty, staff, students, contractors, vendors, guests, volunteers, and others that access servers, workstations, applications or network devices that store, process or transmit MSU data are responsible for complying with these standards.
- MSU Information Security is responsible for monitoring compliance with these standards.

Sanctions:

- Non-compliance with these standards may result in:
  - Disciplinary action, per normal MSU procedures.
  - Revocation of access credentials.
  - Physical or logical removal of non-compliant devices from the MSU network.

Related Standards, Policies, or Procedures:

- MSU Acceptable Use Policy
  - (https://tech.msu.edu/about/guidelines-policies/aup/)
- MSU Institutional Data Policy
  - (https://tech.msu.edu/about/guidelines-policies/msu-institutional-data-policy/)
- NIST 800-53r4
  - (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)
- MSU Information Security Policy
  - (LOCATION TBD)

Additional Resources/ Contact Information:

For more information, please contact the MSU Information Security Governance, Risk & Compliance Team at grc@msu.edu.

Maintenance:

- These standards must be reviewed at least once per year.
- These standards must be revised as necessary.
- This MSU Chief Information Security Officer or their delegate must re-approve these standards after any changes.

Review History:

Date:	Revised By:	Change Summary:
2020.05.18	Ryan M. Finn MSU Information Security Governance, Risk & Compliance	Initial document creation.

Revision History:

Date:	Revised By:	Change Summary:
2020.05.18	Ryan M. Finn MSU Information Security Governance, Risk & Compliance	Initial document creation.

Approval:

Date:	Approved By:	Signature: