Mississippi State University Information Security Program
Risk Assessment and Safeguards

1. **Purpose:** The purpose of this section is to provide a process of identification of information assets in both physical and electronic forms that must be protected and methods to implement safeguards deemed appropriate.

2. **Scope:** The risk assessment program must pertain to all information assets of the institution. The program includes risk management where an ongoing process of risk identification and the subsequent development of plans to safeguard information can be done on a university-wide basis.

3. **Program:** The program must apply a strategic approach to making the university culture evolve into a "risk aware" culture. The complete information security program includes diverse elements such as awareness and training that are in themselves important risk components. The risk assessment process is primarily a management issue that must be addressed by all university personnel whose role includes the management of information wherever it is stored. The State of Mississippi Enterprise Security Policy (ESP) requires an IT security risk assessment from third-party security consultants at least once every three years. MSU's program will meet or exceed the requirements outlined in the ESP Comprehensive Assessment Guidelines.

    - Apply the MSU Data Classification standards to classify institutional information, regardless of media, such as databases, networks, servers and information systems to identify critical systems, assets and risks.

        - Ongoing risk assessment program will include an online risk assessment instrument distributed regularly to correlate the classification and security of information spread throughout the institution.
        - Units must keep an inventory of all server systems and register them with Information Technology Services.
        - A yearly external IT risk assessment for critical units will be focused on providing a comprehensive assessment of all campus within a 3-year period.
        - Penetration testing must be an integral part of external/internal assessments. Proactive social engineering risk analysis will be included.
        - Existing Social Security number usage forms required as per OP 01.23 will be evaluated to confirm system classifications on an ongoing basis.
        - The integrity of MSU's IT environment can be compromised by malicious software running on computer systems

connected to the University's network. Foreign software that is neither commercially available nor open source is high risk and prohibited on university-owned equipment.
Requests for exceptions can be initiated by completing the Foreign Software Exception Form available in Appendix D. A list of approved exceptions is available at the Information Security website infosecurity.msstate.edu.

- Implement Baseline Security Strategies

    - Promulgate to the campus community minimum security standards for computer systems, see Appendix A.
    - Identify current protection strategies such as campus firewall deployments, anti-virus solutions, intrusion detection and staff operational practices that can provide baseline security.
    - Firewall and other protection strategies will be correlated with the campus system inventory and data classifications.

- Identify Infrastructure Vulnerabilities

    - Identify the systems and physical exposure issues in administrative offices and campus computer systems.
    - Proactive vulnerability scans will be performed on all systems that have requested firewall exceptions and additional systems based on information classifications.
    - A robust internal vulnerability assessment program of monthly scans for all Category I servers will be managed by Information Technology Services. Systems change over time and new vulnerabilities are always being discovered requiring an ongoing internal program of vulnerability assessment confirmed by yearly external review.
    - Periodic monthly results summaries will be delivered to relevant campus units.

- Perform Risk Analysis and Mitigation/Safeguards

    - Strategic planning based on the results of the risk assessment allows the targeted implementation of safeguards to systems that contain critical institutional information and where legal requirements are paramount.
    - Two factor authentication is required for web access to all systems storing, processing, or transmitting Category 1 data, and strongly recommended for all other systems.
    - Apply a cost-benefit analysis to the strategic questions of security safeguards and business processes.

- The diverse nature of computing on campus provides for a variety of environments where the application of industry best practice can mitigate risk.

4. **Summary:** Technology alone cannot ensure a secure environment. Personal responsibility, application of good security practice and a University culture that is aware of the risks associated with information breaches can mitigate many security problems. Ongoing risk assessment is a critical component of a complete security program that should change and evolve as the computing and information assets of the institution grow.