Mississippi State University Information Security Program
Monitoring

1. **Purpose:** Security monitoring is the collection, analysis, and escalation of indications and warnings to detect and enable response to breaches of information security. It is also a method of confirming that existing security practices and controls are effective over time. Security monitoring consists of activities such as the review of user account logs, application logs, data backup and recovery logs, automated intrusion detection system logs, and operational procedures. The purpose of security monitoring is to ensure that information resource security controls are in place, are effective, and are not being bypassed.

2. **Scope:** This program applies to the following categories of security:

    - Computer system and application security: Central processing unit, peripherals, operating system software, application software, and data.
    - Physical security: The premises occupied by information technology personnel and equipment as well as storage facilities for analog or digital data.
    - Operational security: Environmental control, power equipment, operational activities.
    - Procedural security: Established and documented security processes for information technology staff, vendors, management, and individual users.
    - Network security: Communications equipment, personnel, transmission paths, and adjacent areas.
    - This program applies to all university information resources.

    The intended audience for this program consists of all data managers/owners and all individuals that are responsible for the installation of new information resources or the operation of existing information resources.

3. **Program:** Security monitoring of information resources shall be implemented based on risk management decisions made by the information resource manager/owner.

    - Category I and Category II information resource systems shall, at a minimum, have operating system and application logging features enabled.
    - Automated tools shall be used where deemed beneficial by the resource owner based on risk management decisions.

- Operating system and application software logging processes shall be enabled on all host and server systems containing Category I or Category II data. Where possible, alarm and alert functions, as well as logging and monitoring systems shall be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a security intrusion or other anomaly is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.
- All network attached systems should have a supported operating system installed which is current with all security patches. Obsolete or unsupported systems shall not be used for communication beyond the local network.
- Regular system integrity checks of host and server systems housing high risk university data should be performed.
- Category III information resource systems are not required to be monitored, but owners of the resources are encouraged to take all appropriate measures to secure them.
- Network security monitoring for the campus backbone network and for departmental networks operated by Information Technology Services will be conducted by ITS. Ancillary networks not operated by ITS must be monitored by the owner/manager of that resource.
- Logs and other data generated by security monitoring shall be reviewed periodically.
- Any significant security issues discovered and all signs of unauthorized activity shall be reported using the procedures detailed in the appropriate section of the Information Security Plan.

4. **Summary:** The assessment of potential risks, the application of appropriate mitigation measures, and the monitoring of these security measures are the responsibility of the information resource manager/owner or their designee.