Mississippi Department of Information Technology Services
Information Security Division
State of Mississippi Enterprise Security Policy

Title 36: Technology

Part 1 Enterprise Security Policy

Part 1 Chapter 1: Security Program Policies

Rule 1.1 Authority
To fulfill the statutory requirements for cybersecurity, the State of Mississippi will have a comprehensive cybersecurity program (the Enterprise Security Program) to provide coordinated oversight of the cybersecurity efforts across all state agencies, including cybersecurity systems, services, and the development of policies, standards and guidelines.

The Mississippi Department of Information Technology Services (ITS) administers the Enterprise Security Program to execute the duties and responsibilities of the Program which includes establishing, maintaining, and oversight of the enterprise security policies and standards for state data and information technology resources.

Source: Miss. Code Ann. § 25-53-201.

Rule 1.2 Purpose
The goal of this policy is to improve the cybersecurity posture of the State by establishing requirements for preserving the confidentiality, integrity, and availability of State of Mississippi information and information technology (IT) systems (hereafter referred to collectively as "SOM Assets") from unauthorized use, access, disclosure, modification, or destruction.

Confidentiality ensures that information is accessible only to those authorized to have access. Integrity ensures the accuracy and completeness of the data is safeguarded. Availability ensures that authorized users have access to the information.

This policy establishes minimum security requirements that all agencies will adhere to, using them as minimum standards with which to develop, implement, and maintain their individual agency IT security policies, plans, and procedures as well as the standards and policies for all state data and information technology resources that state agencies shall implement to the extent

that they apply including defined enterprise security minimum requirements for procuring data and information technology systems and services.

Source: Miss. Code Ann. § 25-53-201.

Rule 1.3 Scope
This policy applies to all state agencies; State of Mississippi employees; ITS trusted partners (e.g., subcontractors, vendors, third-parties, temporary workers, *etc*.); or any entity, as provided by law, authorized to operate, manage, or use SOM Assets. Agency is defined as and includes all the various state agencies, officers, departments, boards, commissions, offices, and institutions of the state.

A. This policy includes a subset of technical requirements that are only applicable to agencies participating in the Enterprise State Network. Agencies that do not participate in the Enterprise State Network, and thus do not have the benefit of the technical controls in place, must develop agency-specific security policies that are:
    1. Appropriate to their respective environments and information, and
    2. Consistent with the intent of this policy.

B. This policy addresses information regardless of what form it takes (i.e., electronic, printed, *etc*.), what technology is used to handle it, the location of the data or resources, or what purpose(s) it serves.

C. This policy encompasses all data and information technology resources (i.e., data and information technology systems (automated and manual), services, products, *etc*.) for which the agencies have administrative responsibility, including data and information technology resources managed, provided, and/or hosted by third parties on behalf of the agencies.

D. Beyond the requirements of this policy, state agencies must also comply with other applicable security standards and policies for state data and IT resources established by ITS. This includes, but is not limited to, the State of Mississippi Enterprise Cloud and Offsite Security Policy, which outlines additional security requirements for cloud and offsite hosting services. Additional policies, requirements, and/or recommendations for state agencies can be found on the ITS website.

Source: Miss. Code Ann. §§ 25-53-3 (2)(e) and 25-53-201.

Rule 1.4 ITS Chief Information Officer
The ITS Chief Information Officer is also the ITS Executive Director. The ITS CIO (or any currently designated acting CIO) oversees all agency activities and ensures that an organizational structure is in place for overseeing security risk management.

Source: Miss. Code Ann. § 25-53-201.

Rule 1.5 Enterprise Security Program
The Enterprise Security Program is focused on providing the resources, guidance, and oversight needed for improving the cybersecurity posture of the enterprise network for state government. ITS has designated a Chief Information Security Officer (CISO) to manage the program and

develop, maintain, and communicate the State of Mississippi Enterprise Security Policy and State of Mississippi Enterprise Security Standards. The ITS CISO and ITS cybersecurity professionals will execute the Program mission by:

A. Administering the Enterprise Security Program to execute the statutory duties and responsibilities of ITS.

B. Researching and selecting enterprise technology solutions capable of improving the cybersecurity posture in the function of any agency, institution, or function of state government as a whole.

C. Establishing and maintaining the security standards and policies for all state data and IT resources that state agencies shall implement, to the extent that they apply.

D. Coordinating and promoting efficiency and security with all applicable laws and regulations in the acquisition, operation, and maintenance of state data, cybersecurity systems, and services used by agencies of the State.

E. Managing, planning, and coordinating all enterprise cybersecurity systems under the jurisdiction of the state.

F. Developing, in coordination with state agencies, enterprise cybersecurity systems and services for all governmental organizations within the purview of ITS.

G. Providing ongoing analysis of enterprise cybersecurity systems and services costs, facilities, and systems within state government.

H. Organizing an advisory council of Information Security Officers from each state agency and coordinating the activities of the advisory council to provide education and awareness, identify cybersecurity-related issues, set future direction for cybersecurity plans and policy, and provide a forum for inter-agency communications regarding cybersecurity.

I. Requiring a cooperative effort for the utilization of enterprise cybersecurity systems and services among MS state agencies.

Source: Miss. Code Ann. § 25-53-201.

Rule 1.6 Agency Heads

The Executive Director and/or Agency Head of each state agency is solely responsible for the security of all data and IT resources under said agency's purview, irrespective of the location of the data or resources. Locations include data residing at agency sites, on agency real property and tangible and intangible assets; in the State Data Centers; in transit between locations; or at a third-party location on behalf of the agency. The Executive Director/Agency Head will ensure that an organizational structure is in place for overseeing security risk management, but is ultimately accountable for:

A. Ensuring that an agency-wide cybersecurity program is in place.

B. Designating an information security officer to administer the agency's security program.

C. Ensuring the agency adheres to the requirements established by the Enterprise Security Program, to the extent that they apply.

D. Participating in all Enterprise Security Program initiatives and services in lieu of deploying duplicate services specific to the agency.

E. Developing, implementing, and maintaining written agency policies and procedures to ensure the security of data and IT resources.

    1. The agency policies and procedures are confidential information and exempt from public inspection, except that the information must be available to the Mississippi's Office of the State Auditor and/or ITS in performing auditing duties.

F. Implementing policies and standards to ensure that all of the agency's data and IT resources are maintained in compliance with state and federal laws and regulations, to the extent that they apply.

G. Implementing appropriate cost-effective safeguards to reduce, eliminate, or recover from identified threats to data and IT resources.

H. Ensuring that internal assessments of the security program are conducted.
    1. The results of the internal assessments are confidential and exempt from public inspection, except that the information must be available to the Mississippi's Office of the State Auditor and/or ITS in performing auditing duties.

I. Including all appropriate cybersecurity requirements in the specifications for the agency's solicitation of state contracts for procuring data and information technology systems and services.

J. Including a general description of the security program and future plans for ensuring security of data in the agency long-range information technology plan.

K. Participating in annual information security training designed specifically for the agency head to ensure that the agency head has an understanding of: the information and information systems that support the operations and assets of the agency; the potential impact of common types of cyber-attacks and data breaches on the agency's operations and assets; how cyber-attacks and data breaches on the agency's operations and assets could impact the operations and assets of other state agencies on the Enterprise State Network; how cyber-attacks and data breaches occur; steps the executive director or agency head and agency employees should take to protect their information and information systems; and the annual reporting requirements required of the executive director or agency head.

Source: Miss. Code Ann. § 25-53-201.

Rule 1.7 Agency Cybersecurity Programs

Agencies must develop and maintain an agency-wide cybersecurity program to address security for information and information systems that support the operations and assets of the agency, including those provided or managed by another organization, contractor, or other source. Agency controls in the management of the cybersecurity program include:

A. Ensuring that an agency-wide cybersecurity program plan is developed, disseminated, and maintained.

B. Ensuring the resources needed to implement the cybersecurity program are documented and available.

C. Developing, monitoring, and reporting on the results of security measures of performance.

D. Ensuring the information technology architecture is designed with consideration for information security and the resulting risk to agency operations, agency assets, individuals, other organizations, and the State.

E. Providing insider threat awareness training to detect and prevent malicious insider activity.

F. Establishing an information security workforce development and improvement program.

G. Developing and maintaining a process for conducting security testing, training, and monitoring activities.

H. Ensuring participation with the Enterprise Security Program to assist the agency with
    1. Facilitating ongoing security education and training for agency employees.
    2. Maintaining knowledge of recommended security practices, techniques, and technologies.
    3. Sharing current security-related information including threats, vulnerabilities, and incidents with appropriate stakeholders.

Source: Miss. Code Ann. § 25-53-201.

Rule 1.8 Agency Information Security Officer

Each agency must designate an Information Security Officer (ISO) that will manage information security tasks and activities within the agency. The ISO responsibilities include:

A. Providing oversight of the agency-wide cybersecurity program within their agency.

B. Collaborating with agency staff on the development, implementation, and maintenance of agency-specific security plans, policies, and procedures.

C. Ensuring that their agency is adhering to the State of Mississippi enterprise security policies and standards; agency-specific policies; and any other security policies, guidelines, regulations, or laws (Federal, State, and Local) their agency is required to comply with.

D. Ensuring that regular assessments and evaluations of the agency's security posture are performed.

E. Recommending a course of action where security risks are not adequately addressed.

F. Reporting security compliance status and advising the agency head and the agency Chief Information Officer (CIO) on the completeness and adequacy of agency security measures.

G. Monitoring and reporting the performance of security measures within their agency.

H. Ensuring all information as required in State of Mississippi enterprise policies and standards are developed and submitted.

I. Ensuring agency participation in the Enterprise Security Program activities, Security Council meetings hosted by ITS, and other security-related activities organized by ITS.

Source: Miss. Code Ann. § 25-53-201.

Rule 1.9 Agency Staff Roles and Responsibilities

All agency staff are personally responsible for information security. The roles and responsibilities of staff must be defined in local policies and procedures and incorporated into the staff orientation process.

A. Agency staff must comply with this State of Mississippi enterprise and agency-specific security policies, standards, and procedures to maintain the confidentiality, integrity, and availability of SOM assets.

B. Agency staff designated as an owner of an agency information system are responsible for the overall procurement, development, integration, modification, or operation and maintenance of information systems including:
    1. Advising the agency on system security categorization.
    2. Ensuring the creation of required system security plans.
    3. Ensuring the implementation of all required security controls for the system.

Source: Miss. Code Ann. § 25-53-201.

Rule 1.10 Policy Framework

This policy is designed to be in alignment with security requirements recommended by the National Institute of Standards and Technology (NIST), the National Cybersecurity and Infrastructure Security Agency (CISA), and the Center for Internet Security (CIS). This policy addresses the five core functions listed below.

A. Identify – Development of an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

B. Protect – Development and implementation of the appropriate safeguards to ensure the security of SOM assets.

C. Detect – Development and implementation of the appropriate activities to identify the occurrence of a cybersecurity event.

D. Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

E. Recover - Develop and implement the appropriate activities to maintain plans to mitigate and to restore critical infrastructure services that were impaired due to a cybersecurity event.

Source: Miss. Code Ann. § 25-53-201.

Rule 1.11 Policy Compliance and Auditing

A. Each agency shall adhere to the more restrictive policy when conflicts exist between this policy and agency policies.

B. Each agency shall regularly review the level of compliance with this policy, document where compliance with the requirements of this policy is not met and develop a plan for addressing the deficiencies.

C. The following information is provided to clarify the role of the Mississippi Office of the State Auditor (OSA) and the Mississippi Department of Information Technology Services (ITS) in auditing compliance:
    1. The State Auditor will review how well agencies comply with security policies as part of their normal agency information systems auditing activities.
    2. As a component of their standard Information Systems audit process, the State Auditor will consider the State of Mississippi Enterprise Security Policy in the review of the systems, processes, and procedures that they will examine.
    3. The State Auditor may determine a special audit of an agency's information system processing is warranted; in which case they will proceed under their existing authority. Each agency must maintain documentation showing the results of its review or audit and the plan for correcting identified deficiencies. To the extent that the audit documentation includes valuable formulae, designs, drawings, computer source code, object codes or research data, or that disclosure of the audit documentation would be contrary to the public interest and would irreparably damage vital government functions, such audit documentation is exempt from public disclosure.
    4. The State Auditor may request the assistance of ITS in the performance of this normal audit function.
    5. The State Auditor may request and review copies of an agency's IT Security Risk Assessment separately or in conjunction with the normal agency audit process.
    6. The State Auditor may request and review the agency's compliance document that identifies the agency's current compliance level with the State of Mississippi Enterprise Security Policy.
    7. Upon determination of any non-compliance, the State Auditor may instruct the agency and/or ITS to take necessary steps to become compliant.
    8. Agencies should understand that failure to comply with this policy could result in a finding in the agency's audit report from the State Auditor.

D. In addition to complying with this policy, it is the responsibility of each agency to determine whether there are any guidelines, regulations, or laws (Federal, State, and Local) outside this policy they are required to meet. These guidelines, regulations, or laws may include, but are not limited to:
    1. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    2. The Privacy Act of 1974, 5 U.S.C. § 552 a, Public Law No. 93-579
    3. Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
    4. Payment Card Industry Data Security Standard (PCI/DSS)

5. Internal Revenue Service (IRS) Publication 1075
6. Criminal Justice Information Services (CJIS)
7. Miss. Code Ann. § 75-24-29 Breach of Security; Require Notice
8. Children's Internet Protection Act (CIPA)
9. Federal Information Security Management Act of 2002 (FISMA)
10. Miss. Code Ann. § 25-1-111 Prevention of Disclosure by State Agencies of Social Security Numbers
11. Driver's Privacy Protection Act (DPPA)
12. The Fair Credit Reporting Act (FCRA)
13. The Gramm-Leach-Bliley Act (GLBA)
14. Miss. Code Ann. § 25-53-193 National Security on State Devices and Networks Act
15. Children's Online Privacy Protection Act (COPPA)

Source: Miss. Code Ann. § 25-53-201.

Rule 1.12 Maintenance of State of Mississippi Enterprise Security Policies, Standards, Guidelines and Recommendations

The revision date for this policy is Month/Day/Year.

A. ITS is responsible for routine maintenance and review of this policy. Routine maintenance and review is required to ensure that this policy is up-to-date with respect to the technological advances and changes in the business requirements of state agencies, potential threats, applicable legislation and other changes that impact information security policies, standards, guidelines and recommendations.

Source: Miss. Code Ann. § 25-53-201.

Rule 1.13 Exceptions to the State of Mississippi Enterprise Security Policies, Standards, Guidelines, and Recommendations

A. The only permitted exceptions to the State of Mississippi Enterprise Security Policy are those that are approved in writing by ITS for an agency's specific purpose and are only applicable to that agency's operations for the duration of time defined by the exception.

B. Each agency must inquire with the agency partner (e.g., subcontractor, vendor, third-party, *etc*.) and appropriate agency staff to ascertain if design alternatives, configuration changes, or additional products, systems, or services are available to attain compliance prior to submitting a request for an exception.

C. Prior to selecting, acquiring, and/or procuring data and information technology resources (i.e., data and information technology systems, services, products, *etc*.) and/or renewing existing agreements for data and information technology resources, each agency must consider all applicable enterprise policies and standards and is responsible for ensuring the data and information technology resource allows the agency to be in compliance with all applicable enterprise policies and standards when specifying, scoping, evaluating, and/or renewing solutions and that all appropriate

cybersecurity requirements are included in the acquisition/procurement of data and information technology solutions.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 2: Asset Management

Rule 2.1 System and Physical Device Inventory

A. Each agency must maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This should include all assets with an IP address.
    1. Implement a process that requires approval before new assets are installed or deployed. This process shall include the designation of a person, or persons authorized to make such approvals, and documentation describing how these approvals are recorded.
    2. The inventory shall include all hardware assets, whether connected to the agency's network or not. This includes agency assets owned, operated, or managed by a third party.
    3. The inventory shall be maintained and updated throughout the asset's lifecycle (installations, removals, updates, *etc*.).
        i. Unsupported assets/hardware that can no longer receive security patches must be removed from the network.
    4. The inventory information for each asset should include the network address (if static), hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network. For assets with dynamic addresses provided by DHCP, refer to ITS's recommendation on utilizing DHCP.
        i. ITS recommends utilizing dynamic host configuration protocol (DHCP) logging on all DHCP servers or IP address management tools to update the agency's hardware asset inventory. Agencies might consider creating DHCP reservations for all systems with dynamic addresses in order to keep addresses from changing frequently.
    5. ITS recommends maintaining active ports, services, and protocols to the hardware assets in the asset inventory. Agencies might utilize port scanning on a regular basis to review all open ports, identify any unauthorized ports, and develop this portion of the inventory.

B. Each agency must ensure that unauthorized assets are either removed from the network or receives a documented exception.
    1. Employing MAC-based ACL's or other methods are highly encouraged to prevent an unauthorized host from connecting to the network. If this can be employed, reviews should be performed regularly to ensure that it is working as intended. If such technical controls cannot be implemented, network scans should be executed on a frequent basis to identify unauthorized hosts.

C. ITS recommends utilizing an active discovery tool, such as a network port scanner, for updating the hardware asset inventory.

D. ITS recommends utilizing dynamic host configuration protocol (DHCP) logging on all DHCP servers or IP address management tools to update the agency's hardware asset inventory. Agencies might consider creating DHCP reservations for all systems with dynamic addresses in order to keep addresses from changing frequently.

E. ITS recommends deploying automated mechanisms to support tracking and recovery of physical devices and systems.

Source: Miss. Code Ann. § 25-53-201.

Rule 2.2 Software Inventory

A. Each agency must maintain an up-to-date list of all authorized software that is required for any agency purpose on any agency system.
    1. Implement a process that requires approval before new software is installed or deployed.
    2. Software platform and application inventory shall be maintained and updated throughout the asset's lifecycle (installations, removals, updates, *etc*.).

B. Each agency must ensure that software, applications, or operating systems that have reached EOL and are no longer supported are replaced with alternatives which are supported by its respective vendor. This does not apply to in-house software development unless third-party tools or components are included within its design or functionality.
    1. Unsupported software should be removed from the authorized software inventory system or at least "No longer authorized for use on agency systems".

C. Each agency must ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. This should be reviewed on a regular basis, or at least monthly.

D. ITS recommends utilizing software inventory tools throughout the agency to automate the documentation of all software on agency systems.
    1. The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the agency.

E. ITS recommends utilizing technical controls, such as application allowlisting (application control), to ensure that only authorized software can execute or be accessed. The functionality of these controls should be reviewed bi-annually, *at minimum*.

F. ITS recommends utilizing technical controls to ensure that only authorized software libraries (such as .dell,, .ocx,, .so files) are allowed to load into a system process. Block unauthorized libraries from loading into a system process. The functionality of these controls should be reviewed bi-annually, *at minimum*.

Source: Miss. Code Ann. § 25-53-201.

Rule 2.3 Classification of Information Assets

A. Each agency must establish a framework for classifying information[1] based on its sensitivity and criticality to the agency.
    1. The framework applies to all data created, collected, accessed, owned, processed, maintained, stored, or transmitted by the agency and covers all employees, contractors, and third-party users who have access to this data.

B. Each agency shall serve as a classification authority for its information and information assets irrespective of location, resource, or form. This includes information and/or information assets managed or hosted by third parties.

    1. Data classifications are a prerequisite to establishing agency policies and guidance regarding the collection, generation, access, processing, storage, maintenance, transmission, archiving, and disposal of state data.

        i. In addition to the data classification requirement, ITS recommends all data have a designated data owner responsible for the identification and classification of the information they have been designated as well as establishing rules for data governance and that appropriate requirements are incorporated into agreements relating to the agency's classified data.

C. Each agency must classify data based on potential impact to the agency's ability to accomplish its assigned mission, fulfill its legal responsibility, maintain its day-to-day functions, and protect individuals that would be caused by a loss of confidentiality, integrity, or availability of the data.
    1. Confidentiality
        i. Preserving authorized restrictions on information access and disclosure, including means for protecting person privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
    2. Integrity
        i. Guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
    3. Availability
        i. Ensuring timely and reliable access to and use of information. A loss of availability is a disruption of access to or use of information or an information system.

D. Each agency must classify data into one of three categories: Low, Moderate, and High. These categories are based on the potential impact on the agency should the data be compromised in terms of confidentiality, integrity, or availability.
    1. Low

[1] The use of the words "information" and "data" are interchangeable.

i. The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on agency operations, agency assets or individuals.

2. Moderate
    i. The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on agency operations, agency assets or individuals.
3. High
    i. The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on agency operations, agency assets or individuals.

E. Each agency must maintain an inventory of all data created, collected, accessed, stored, processed, or transmitted by agency assets, including those located on-site or at a remote service provider, classified as Moderate or High.

    1. ITS recommends agencies also maintain data mapping of on-premise and off-premise systems, servers, applications, *etc*. that have data classified as Moderate or High.

F. Each agency must determine if their information and information systems are subject to state or federal legal requirements and categorize them as required by law (i.e. HIPAA, PCI, IRS, CJIS, *etc*.).

G. Each agency must establish a process to regularly review and adjust the appropriateness of assigned classifications throughout the lifecycle of the data.

H. Each agency must ensure that data classified as Moderate or High is secured in accordance with applicable agency requirements, federal or state regulations/guidelines, and the enterprise security policy.

I. Each agency must ensure that data shared, as permitted by applicable legal requirements, with any other public or private entity is classified and protected in accordance with agency and applicable legal requirements and in accordance with a document agreement detailing, *at minimum*, data treatment and protection requirements.

J. All reproductions of information in its entirety must carry the same information classification as the original. Partial reproductions of information need to be evaluated to determine if new classifications are warranted.

K. If an agency is unable to determine the classification of specific data sets, the data should be assigned a classification that is equivalent to the highest classified data in the set.

L. ITS recommends all personally identifiable information (PII) be classified, *at minimum*, as “Moderate”.

M. Agencies must adhere to all applicable privacy laws, regulations, policies, and procedures regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII.

N. Additionally, agencies must establish administrative, technical, and physical safeguards to protect PII from unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

O. ITS recommends agencies consider implementing the below recommendations as it relates to PII.

1. Agencies should only create, collect, use, process, store, maintain, disseminate, and/or disclose PII if they have legal authority to do so.
    i. Additionally, agencies should, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII.
2. Agencies should only create, collect, use, process, store, maintain, disseminate, and/or disclose the minimum amount of PII that is relevant and necessary to accomplish its assigned mission, legally authorized purpose, maintain its day-to-day functions, and fulfill its legal responsibility.
3. In addition to establishing safeguards to protect PII as required in Rule 2.3(M), agencies that create, collect, use, access, process, maintain, share, disseminate, disclose, and/or store PII should also develop policies, procedures, and processes aligned with applicable legal requirements and privacy principles and best practices that address the preceding as well as purpose, retention, and disposal of PII.
4. Agencies should be transparent and provide notice to individuals regarding the creation, collection, use purpose, processing, storage, maintenance, dissemination, disposal, and disclosure of PII.
    i. Agencies should only use PII for the purpose(s) specified in the notice.
5. Agencies should ensure PII is accurate, relevant, timely, and complete.
6. Agencies should only maintain PII for as long as legally required and/or necessary to accomplish its purpose and/or mission.
7. Training should be provided to all parties with access to and/or who use/process PII.
8. Agencies should consider the Fair Information Practice Principles (FIPPs) and/or NIST Privacy Framework when evaluating products, systems, services, solutions, processes, programs, risks, and activities involving PII and/or affecting individual privacy.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 3: Governance

Rule 3.1 Security Policies

A. Each agency must develop, implement, and maintain their individual agency IT security policies.

B. Each agency must incorporate requirements from the State of Mississippi Enterprise Security Policy as minimums in their agency security policies.
    1. Each agency will annually review and revise (as needed) its security policies.
        i. Revisions to agency security policies must incorporate relevant technological advances in the broad areas of IT, changes in agency business requirements, and changes in the agency's IT environment.

Source: Miss. Code Ann. § 25-53-201.

Rule 3.2 Cybersecurity Program

A. Each agency must develop and implement an agency-wide cybersecurity program plan. All agency personnel should have an understanding of the cybersecurity program; however, the level of detail may vary depending on the employee's role and the sensitivity of the information.
    1. The plan shall describe the agency's current security posture, include an assessment of current risk, and a plan of action and milestones that describe current gaps in the security program and summarize the goals of the agency to address those gaps.
    2. The plan shall include the assignment of roles and responsibilities, including the contact information for the designated agency Information Security Officer.
    3. Each agency must provide a letter of compliance as a component of its cybersecurity program plan which describes applicable State, Federal, and Local regulations, laws, and standards it is required to satisfy. This includes compliance with the State of MS Enterprise Security Program.
        i. Letters of compliance must be signed by the agency head, who is responsible for the oversight of IT security. Letters of compliance must indicate that the agency head has observed, reviewed, and approved agency security processes, procedures, and practices.
    4. Each agency must annually review and revise (as needed) its cybersecurity program plan to reflect relevant changes that impact the plan.

B. Each agency must have a security program maturity assessment performed at least once every two (2) years. This assessment will determine the current level of compliance with the State of MS Enterprise Security Policy, identify security threats to their environment, and learn about remediation opportunities that may help to strengthen their ability to protect SOM assets from cyberthreats.
    1. The program assessment must utilize an ITS-defined set of criteria to evaluate the effectiveness of the agency security program and the controls that protect the assets that support the agency.
    2. The results of the assessment must be provided to ITS.
    3. The cybersecurity program maturity assessment must be performed by an ITS-approved third-party cybersecurity assessment provider and can be included as part of the required comprehensive cybersecurity assessment as defined in the cybersecurity assessment chapter of this policy.

Source: Miss. Code Ann. § 25-53-201.

Rule 3.3 Legal and Regulatory Requirements

A. Each agency must ensure that all applicable State and Federal legal and regulatory requirements regarding cybersecurity and information privacy and security are understood, addressed, and satisfied.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 4: Access Control

Rule 4.1 Access Management

A. Each agency must limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). For implementation, ensure that each asset has strong user authentication as well as network and local access control lists necessary to implement "need-to-know" and "least privilege".
    1. Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, modifying access, or role change of a user.
        i. All access to enterprise assets must be authenticated and adhere to guidance that follows; and
        ii. All granting of account access (assignment of privileges) must follow a strict and defined process (i.e. using account request forms and approvals thereof by the appropriate personnel). This process is preferably automated (such as the use of Privileged Access Management (PAM) systems) but can also be manual.
    2. Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.
    3. Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.
        i. For implementation, consider having respective department heads or other appropriate persons review user accounts lists provided by system administrators for each asset within the Enterprise. Any noted necessary changes should be provided to the system administrator and another account listing should be generated for subsequent review and confirmation the actions were taken.
    4. Require users to authenticate to enterprise-managed VPN prior to accessing enterprise resources on end-user devices.
    5. ITS recommends deploying port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

        i. 802.1x is preferred as it gives the greatest level of security and flexibility. However, if this is not possible, ITS recommends configuring "sticky MAC" or simply limiting the MAC address that can be used for a particular network port, especially in areas where the connected network devices do not change frequently.

B. Each agency must limit system access to the types of transactions and functions that authorized users are permitted to execute.
    1. Establish and follow a process, preferably automated, for revoking access to SOM assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. If an automated system cannot be implemented, ITS recommends documenting a manual checklist that is part of the HR process.
    2. Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.
        i. ITS recommends that this review be conducted in conjunction with the review described in Part 1, Chapter 4, Section A.3.
    3. Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.
    4. Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.
    5. ITS recommends defining and maintaining role-based access control, through determining and documenting the access rights necessary for each role within the agency to successfully carry out its assigned duties. Perform access control reviews of SOM assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.
        i. Note that if the agency is utilizing the ITS-managed Enterprise VPN solution, this control will be implemented as part of that service.

C. Each agency must control the flow of sensitive data in accordance with approved authorizations.
    1. Document data flows. Data flow documentation includes service provider data flows into and out of the organization and should be based on the organization's data management process. Within that diagram, the organization should include mechanisms (such as firewalls) that filter the flow of data, encryption devices that protect the data, and intrusion detection systems that analyze the data.
        i. Review and update documentation annually, or when significant enterprise changes occur that could impact this safeguard.
    2. An authoritative figure should be designated to review and approve changes to data flow prior to their implementation.

D. Each agency must separate the duties of individuals to reduce the risk of malicious activity without collusion.
    1. ITS recommends defining and maintaining system access authorizations, such as roles or user groups with differing permissions, to support separation of duties. Perform authorization reviews, on a recurring schedule at a minimum annually, or more frequently.

E. Each agency must employ the principle of least privilege, including for specific security functions and privileged accounts.
    1. Establish and maintain a secure network architecture. A secure network architecture must address segmentation (using implementation methods such as VLAN access controls and/or firewalls to segment and protect systems), least privilege (ensuring users only have access to the systems and data required for their job), and availability (using redundant systems and data paths), at a minimum.

F. Each agency must use non-privileged accounts or roles when accessing non-security functions or roles for general computing activities, such as Internet browsing.
    1. ITS recommends administrator privileges to dedicated administrator accounts on SOM assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

G. Each agency must prevent non-privileged users from executing privileged functions and audit the execution of such functions.
    1. ITS recommends logging sensitive data access, including modification and disposal.

H. Each agency must limit unsuccessful logon attempts.
    1. Enforce automatic account lockout following a predetermined threshold of local failed authentication attempts.
    2. The account should be locked until released by an administrator or until a specified period of time has passed. The decision for release of an account after exceeding the threshold of failed authentication attempts should be based on capabilities of the account.

I. Each agency must ensure that systems have screen locks or password protected screen savers which are activated after a defined period of inactivity.
    1. Configure automatic session locking on SOM assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.

J. Each agency must terminate (automatically) a user session after an agency-defined condition or trigger events requiring session disconnect.
    1. Examples of conditions or trigger events requiring automatic session termination could include defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use.

K. Each agency shall display a system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Source: Miss. Code Ann. § 25-53-201.

Rule 4.2 Remote Access Management

A. Each agency must terminate all VPNs in the Enterprise VPN Solution managed by ITS.
    1. Agencies can request an exception to this requirement for the following:
        i. Terminating one or more VPNs using another method other than the Enterprise VPN Solution.
        ii. Accessing a Virtual Desktop Infrastructure from the Internet without a VPN.
    2. Agencies are required to provide documentation that justifies that the exception is required for meeting applicable security compliance requirements.
    3. In any case where ITS approves an exception, the exception only applies to a singular VPN, unless otherwise specified, and said VPN must be built to meet or exceed all controls specified within the Enterprise Security Policy.

B. All connections from any entities (state or third party) that reside on the outside of the Enterprise State Network must be made via a virtual private network (VPN) connection (using industry-standard IPSec or SSL protocols) or via a third-party circuit that terminates at the ITS data centers in a DMZ on the Enterprise Perimeter Firewall.
    1. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the agency's secure configuration process, and ensuring the operating system and applications are up-to-date.
    2. Require multi-factor authentication for remote network access.
    3. Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.

C. All connections from any entities (state or third party) that reside on the outside of the state network must be made via a virtual private network (VPN) connection using industry-standard IPSec or SSL protocols.

D. VPNs may be client-based or LAN-to-LAN based.
    1. Client-based VPNs are VPNs in which software (client) is installed on a remote user's computer and a secure connection is made between that VPN client and a VPN-capable terminating device (i.e. VPN concentrator, firewall, router, server).
        i. All client-based VPNs must require multi-factor authentication.
    2. LAN-to-LAN VPNs are VPNs that are created between a VPN-capable device on a third-party network and a VPN-capable device on the state network.

E. For client-based VPNs, split-tunneling must be disabled on any device (firewall, VPN Concentrator, *etc*.) used to terminate VPNs inside the state network.
    1. Split tunneling is defined as having the ability to participate in a LAN while connected to the state Network via VPN. To meet the requirement of disabling split tunneling, it is required that all network activity for the client PC be redirected down the tunnel. Both listening services and browsing services must be redirected to the VPN so that no LAN activity can take place, regardless of whether it is initiated by the client PC or by another device on the LAN.
    2. Any device (including SSL VPN appliances) that cannot fully disable split tunneling as it is defined above does not meet the requirements or intent of this security policy.

F. All remote access across any network, internal or external to the agency environment, must employ cryptographic mechanisms to protect sensitive data.

G. For both client-based and LAN-to-LAN VPNs, tunnels must be limited with access-restrictions that are granular enough to restrict all inbound traffic to both IP addresses and specific TCP/UDP ports. The list of addresses and ports allowed must only include what is necessary for the applications used by the remote users.

H. Authorization for remote execution of privileged commands and remote access to security-relevant information must be limited to agency-defined needs. A privileged command is a human-initiated (interactively or via a process operating on behalf of the human) command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. Security-relevant information is any information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.
    1. To understand and comply with this requirement, each agency should:
        i. Identify privileged commands (or activity) authorized for remote execution.
        ii. Identify security-relevant information that can be accessed remotely.
        iii. With these identified, it is recommended that firewall rules governing remote access be used to enforce these restrictions. Further, users with privileged access should be trained and aware of this policy.

I. All remote access to the Enterprise State Network must be revoked immediately upon the retirement, resignation, dismissal, end of contract, or all other actions that signal that the requirements for having a connection are no longer valid.

J. At no time should any employee, vendor or account holder provide their remote access credentials (user information or password) to anyone. Employees, vendors, or account holders must be assigned individual accounts.

K. All remote access (VPN and other remote access types) must require multi-factor authentication.

Source: Miss. Code Ann. § 25-53-201.

Rule 4.3 Wireless Access

A. Each agency must ensure that all Wireless Local Area Networks (WLANS) are configured securely.
    1. Authorize each type of wireless access prior to allowing such connections by establishing and maintaining a secure configuration process for network devices such as the access point and switches supporting the wireless access.
    2. Protect wireless access using secure network management (TLS, SSH) and communication protocols (WPA2 and WPA3).
    3. Utilize the Advanced Encryption Standard (AES) for wireless access.
    4. Each agency must ensure that their wireless deployment encryption keys are rotated regularly and frequently (at least every 6 months). Further, all encryption keys should be changed if wireless access must be revoked (such as after termination or transfer of an employee).
    5. ITS recommends disabling wireless access on devices that do not have a business purpose for wireless access.
    6. ITS recommends disabling peer-to-peer wireless network capabilities on wireless clients.
    7. ITS recommends configuring wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.
    8. ITS recommends ensuring that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) to provide credential protection and mutual authentication.
    9. ITS recommends disabling wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.

B. Each agency must ensure that guest/public users are not permitted access to the state network resources.
    1. Agencies wishing to provide Internet access to a guest user must utilize one of the following approved methods:
        i. Installing separate equipment and a separate circuit for guest users. Contact ITS for more information on this method of connectivity.
        ii. Tunneling guest user traffic to an ITS DMZ via a wireless controller solution implemented by ITS. Contact ITS for more information on this method of connectivity.
    2. Both methods require:
        i. No ports opened inbound to guest users.
        ii. All guest user traffic must be filtered.

Source: Miss. Code Ann. § 25-53-201.

Rule 4.4 Portable and Mobile Device Access

A. Each agency must ensure that all portable and mobile devices are controlled and configured securely. Portable and mobile devices are computing devices that have a small form factor such that it can easily be carried by a single individual; is designed

to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Portable and mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, laptops, and tablets. These devices are typically associated with a single individual.

1. Where possible, require multi-factor access for portable and mobile devices.

B. Each agency must ensure that all confidential information stored or processed on portable and mobile devices is encrypted (whole-disk encryption, full-device encryption, container-based encryption, *etc*.).
    1. Utilize technology that can remotely wipe portable and mobile devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.
    2. ITS recommends using a management platform that allows central administration of the appropriate security policy to all devices supported by the agency.

C. Each agency must enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on all portable and mobile devices.
    1. For laptops, do not allow more than 20 failed authentication attempts: for tablets and smartphones, no more than 10 failed authentication attempts.

D. Each agency must ensure that any device connected to the Enterprise State Network has only one active connected network interface at any time. For example, if plugged into Ethernet, Wi-Fi is disabled.

Source: Miss. Code Ann. § 25-53-201.

Rule 4.5 External Information Systems

A. Each agency must establish and maintain an inventory of all known service providers approved to access SOM assets or approved to process, store, or transmit SOM data.
    1. The inventory includes classification(s), and the designated enterprise contract(s) for each service provider.
    2. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk.
    3. Review and update the inventory annually, or when significant enterprise changes occur that could impact this safeguard.

B. Each agency must ensure service provider contracts include appropriate security requirements. More details about security requirements for cloud and offsite hosting services are included in the Enterprise Cloud and Offsite Hosting Security Policy on the ITS website.

C. Each agency must control sensitive information that is posted or processed on publicly accessible systems.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 5: Awareness and Training

Rule 5.1 User Awareness Education and Training

A. Each agency must ensure all employees, associates, business partners, and others using SOM systems and data are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems and data.

B. Each agency must implement and maintain a security awareness training program for all agency users (including managers, senior executives, and contractors) to educate them on how to interact with SOM systems and data in a secure manner.
    1. Conduct training at hire and, at a minimum, annually.
    2. Train agency users to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
    3. Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.
    4. Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.
    5. Train workforce members to be able to recognize a potential incident and be able to report such an incident.
    6. Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.
    7. Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.
    8. Ensure that the security awareness program and related content is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.
    9. Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, exposing sensitive data in artificial intelligence models, or publishing data to unintended audiences.
    10. Each agency must determine the method of training, weighing the convenience of computer-based training against the value of live classroom training.
        i. Agencies electing to use computer-based training must adhere to the enterprise standard for security awareness and education training. More information about enterprise standards can be found on ITS's website.

C. Each agency must ensure that users are trained to carry out their assigned cybersecurity-related duties and responsibilities.
    1. Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, advanced social engineering awareness training for high-profile roles, and specific training for personnel who maintain or secure operational technology (OT) as part of their regular duties. OT encompasses the hardware and machines responsible for the physical security processes.
    2. ITS recommends each agency train personnel responsible for IT and OT assets on how to effectively respond to OT cyber incidents.

D. Each agency must provide security awareness training on recognizing and reporting potential indicators of insider threats.

Source: Miss. Code Ann. § 25-53-201.

Rule 5.2 Senior Executives Roles and Responsibilities

A. Each agency head must clearly communicate to senior executives their roles, as well as the responsibilities that accompany those roles.

B. Each agency head must participate in annual information security training designed specifically for the agency head to ensure that the agency head has an understanding of:
    1. The information and information systems that support the operations and assets of the agency.
    2. The potential impact of common types of cyber-attacks and data breaches on the agency's operations and assets.
    3. How cyber-attacks and data breaches on the agency's operations and assets could impact the operations and assets of other state agencies on the Enterprise State Network.
    4. How cyber-attacks and data breaches occur.
    5. Steps the agency head and agency employees should take to protect their information and information systems.
    6. The annual reporting requirements required of the agency head.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 6: Audit and Accountability

Rule 6.1 Audit and Accountability

A. Each agency must create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
    1. Establish and maintain a process for managing audit logs. This process should include documented policy which addresses the sensitivity of the agency's

audit logs, personnel who will retain ownership of audit logs, log handling procedures, and log disposal requirements. Review and update documentation annually, or when significant agency changes occur that could impact this safeguard.

2. Ensure the audit log management process defines the agency's logging requirements. At a minimum, address the collection, review, and retention of audit logs for agency assets.
3. Collect audit logs for all agency assets (especially those processing, storing, or transmitting sensitive data) as defined in the collection requirements of the audit log management process.
4. Ensure that all audit logs, if applicable, include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.
5. Ensure that logging destinations maintain adequate storage to comply with the agency's audit log management process.
6. Collect DNS query audit logs on agency assets, where appropriate and supported.
7. Collect URL request audit logs on agency assets, where appropriate and supported.
8. Collect command-line audit logs, where appropriate and supported. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.
9. Centralize, to the extent possible, audit log collection and retention across agency assets. This ensures security event alerting for all agency assets can be easily correlated and analyzed. An example of this would be a central log server or SIEM that collects and stores all agency asset logs.
10. Ensure that audit logs are maintained based on agency audit log management processes and include a minimum retention of at least 90 days and a maximum retention timeline.
11. ITS recommends logging access to sensitive audit log data, including modification and disposal, to include both the account accessing log data as well as timestamps.
12. ITS recommends collecting service provider logs, where supported. Examples include collecting authentication and authorization events, data creation and disposal events, and user management events.

B. Each agency's use of audit logs must ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.

C. Each agency must conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

D. Each agency must define processes for alerting in the event of an audit logging failure. These processes should include defined actions to be taken when an alert is received. Examples of audit log failures includes events such as log disks becoming

full or corrupted. Examples of alerts could be automated emails to be sent to log management personnel.

E. Each agency must implement a process to review, analyze, and report correlated audit logs for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

F. Each agency must centralize security event alerting across agency assets for log correlation and analysis.
    1. ITS recommends the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this safeguard.

G. Each agency must configure logging to utilize internal system clocks within each agency asset to generate time stamps for audit logs.
    1. Standardize time synchronization across all agency assets. At least two synchronized and authoritative time sources should be used in each agency asset, where supported. Examples of time sources are network time protocol (NTP) time servers. Agencies on the State network have the option of using the ITS time servers (tick.its.ms.gov and tock.its.ms.gov).
    2. ITS recommends implementing a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. Examples of time synchronization services and assets include Windows Time Service (W32Time) and separate, internal Network Time Protocol (NTP) servers.

H. Each agency must protect audit information and audit logging tools from unauthorized access, modification, and deletion.
    1. ITS recommends encrypting logs for maintaining integrity and confidentiality of sensitive data.

I. Each agency must limit management of audit logging functionality to a subset of privileged users. This includes the ability to view, edit, and delete logs, as well as permissions necessary to change logging configurations.
    1. ITS recommends defining and maintaining role-based access control, through determining and documenting the access rights necessary for management of audit logging functionality within the agency. Perform access control reviews of agency assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 7: Configuration Management

Rule 7.1 Configuration Management

A. Each agency must establish and maintain baseline configurations of agency systems (including hardware, software, and firmware) throughout the respective system development life cycles.

B. Each agency must establish and maintain a secure configuration process for agency assets. Review and update documentation annually, or when significant enterprise changes occur.
    1. Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS as opposed to Telnet and HTTP.
    2. Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

C. Each agency must track, review, approve or disapprove, and log meaningful changes to agency systems.
    1. This can be accomplished through a number of ways provided they are fully implemented and utilized for all changes. For example, specialized software packages can be licensed for this purpose or for smaller environments, adequately designed spreadsheets could be utilized. Ultimately, as long as all meaningful changes are tracked, reviewed, and approved, the solution to do this is irrelevant.
    2. Less meaningful changes that the agency determines doesn't need to be reviewed and approved should be logged for historical reference.

D. Each agency must analyze the security impact of changes prior to implementation and ensure documentation is updated.
    1. Any configuration change which is identified as resulting in a meaningful impact to the agency's functionality (i.e. installation of new software or hardware, implementation of new methods for granting or removing access, *etc*.) should be reviewed, its impact considered, and the change documented prior to its rollout.

E. Each agency must review, approve or disapprove, and enforce physical and logical access restrictions associated with changes to agency systems.
    1. These access appointments should be documented or otherwise logged via either logical or physical mediums, such as permission delegation via Active Directory or physical sign-in sheets placed at entry points.

F. Each agency must employ the principle of least functionality by configuring agency systems to provide only essential capabilities.

G. Each agency must uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

H. Each agency must use technical controls (when possible), such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess this allowlist bi-annually *at minimum*, or more often if significant change to software inventory necessitates.

I. ITS recommends using software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 8: Identification and Authentication

Rule 8.1 Identification and Authentication Management

A. Each agency must identify system users, processes acting on behalf of users, and devices. Typically, individual identifiers are the usernames associated with the system accounts assigned to those individuals. Additionally, common device identifiers can include: media access control (MAC), Internet protocol (IP) addresses, device-unique token identifiers.

B. Each agency must establish and follow an authentication process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.
    1. All access to enterprise assets must be authenticated and adhere to guidance that follows; and
    2. All granting of account access (assignment of privileges) must follow a strict and defined process (i.e. using account request forms and approvals thereof by the appropriate personnel). This process is preferably automated (such as the use of Privileged Access Management (PAM) systems) but can also be manual.

C. Each agency must use multifactor authentication (MFA) for local (console or other direct access) and network access (any access that occurs over a network of any type) to privileged accounts and for network access to non-privileged accounts. For network access, this includes such protocols as RDP, SSH, and VDI. Multifactor authentication requires the use of two or more different factors to authenticate. The factors are defined as something you know (e.g., password, personal identification number [PIN]); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric).
    1. Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.
    2. Require all externally exposed agency or third-party applications (such as Box, 365, *etc*.) to enforce MFA, where supported. Enforcing MFA through a directory service or single sign on (SSO) provider is a satisfactory implementation of this requirement. This includes public access to state licensure sites.
    3. Where MFA authentication is not supported (such as local administrator, root, or service accounts), accounts must use passwords that contain at least fourteen (14) characters and are unique to that system. The passwords should be changed when the account is believed to have been breached or otherwise compromised in any way.

D. Each agency must implement replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
    1. Authentication processes resist replay attacks if it is impractical to successfully authenticate by recording or replaying previous authentication messages. For example, Windows systems not in a domain rely on NTLM and NTLMv2 authentication. These protocols are vulnerable to replay attacks. Join workstations to a domain to ensure Kerberos is used as an authentication protocol (which is not vulnerable to replay attacks). As an alternative, use a one-time password authentication mechanism (such as an RSA token) for logging into systems.

E. Each agency must prevent reuse of identifiers for an agency-defined period. For example, when a user leaves an agency, the username assigned to that user should not be re-used for a specified period (such as 6 months).

F. Each agency must disable identifiers after an agency-defined period of inactivity (such as 45 days).

G. Each agency must enforce minimum password requirements for all non-administrator accounts. At minimum, the guidelines must adhere to the detailed guidance in NIST 800-63B section 5.1, 5.1.1.1, 5.1.1.2 and the additional requirements below.
    1. Passwords must be unique per unique account. If one username/account is used across multiple assets, it must employ a unique password on each.
    2. Passwords must contain at least 8 characters for accounts using MFA and 14 characters for accounts not using MFA.
    3. Passwords must not be disclosed to anyone except in emergency circumstances or when there is an overriding operational necessity.
    4. Usernames must be unique per user. Further, "group" or shared accounts should not be utilized.
    5. Default passwords must adhere to the requirements of this section and must be changed upon initial authentication by the user. During account creation or password resets, unique passwords should be set for each account as opposed to using a common, default password for multiple users.
    6. Passwords must be required on all user accounts.
    7. Each agency must prohibit automated/scripted password input.

H. Each agency must use industry-standard encryption standards to encrypt passwords when stored or in transit. At a minimum, encryption shall meet or exceed AES 128-bit and TLS 1.3.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 9: Incident Response

Rule 9.1 Incident Response Management

A. Each agency must establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan.

1. Each agency must ensure that their incident response process is appropriately aligned with the State of MS's Enterprise Cybersecurity Incident Response Plan. The enterprise plan can be found on the ITS website (www.its.ms.gov).
2. Review the incident response process annually, or when significant agency changes occur that could impact this safeguard. This may include changes to network architecture which may affect business continuity, perceived or realized security events, or other modifications to an agency's infrastructure which alter business flow.
3. In addition to maintaining an electronic version of the incident response plan, all agencies must prepare a hard copy which is maintained and accessible to appropriate staff.

B. Each agency must designate one key person, and at least one backup, who will manage the agency's incident handling process.
    1. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the agency to oversee any third-party work. All agencies must document whether incident response is handled internally or via a third-party vendor and shall retain any documentation describing agreements made with external service providers.
    2. Review the management personnel designations annually, or when significant agency changes occur that could impact this safeguard.

C. Each agency must assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. All assignments must be documented as a component of the agency Incident Response plan.
    1. Review key roles and responsibilities annually, or when significant agency changes occur that could impact this safeguard.

D. Each agency must determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident.
    1. Review communication mechanisms annually, or when significant agency changes occur that could impact this safeguard.

E. Each agency must track, document, and report incidents to designated officials and/or authorities both internal and external to the agency.
    1. Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, or other stakeholders. Verify contacts annually to ensure that information is up to date.
    2. Establish and maintain an agency process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure

the process is publicly available to all of the workforce. Review annually, or when significant agency changes occur that could impact this safeguard.

3. Each agency must report all cybersecurity incidents to ITS involving their information and information systems, whether managed by the state agency, contractor, or other source. Please refer to the State of MS's Enterprise Cybersecurity Incident Reporting Guidelines document for more detailed information on reporting cybersecurity incidents and timelines. The document can be found on the ITS website (www.its.ms.gov).

F. Each agency must test the agency incident response capability.
    1. Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.

G. Each agency must conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.
    1. Document the way the incident was identified, actions taken in response to the incident, and any impact to agency resources or functionality incurred as a result of the incident.
    2. Lessons learned from post-incident reviews must be documented and deficiencies must be addressed in a timely fashion. Actions taken to remediate known identified deficiencies must be documented.

H. ITS recommends that each agency establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. A security event is an observed change to the normal behavior of a system, environment, process, workflow, or person. Examples of events may include router ACLs were updated; firewall policy was pushed. An incident is an event that negatively affects the confidentiality, integrity, and/or availability in a way that impacts the agency. Examples: attacker posts company credentials online, attacker steals customer credit card database, worm spreads through network.
    1. Review the post-incident process annually, or when significant agency changes occur that could impact this safeguard.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 10: Maintenance

Rule 10.1 Maintenance Management

A. Each agency must establish and maintain procedures and processes for performing maintenance on agency IT systems.
    1. Ensure all potentially impacted security controls are still functioning properly following maintenance, repair, or replacement actions.

2. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location.

B. Each agency must approve, control, and monitor the use of system maintenance tools.

C. Each agency must ensure equipment removed for off-site maintenance is sanitized of any sensitive or confidential information.

D. Each agency must assess media containing diagnostic and test programs for malicious code before the media are used in agency IT systems.

E. Each agency must require multifactor authentication to establish maintenance sessions via external (nonlocal) network connections and terminate such connections when maintenance session is complete.

F. Each agency must supervise the maintenance activities of maintenance personnel without required access authorization.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 11: Media Protection

Rule 11.1 Media Protection

A. Each agency must protect (i.e., physically control and securely store) all sensitive stored data, both hard copy and digital media, on all systems (agency-managed and hosted). All sensitive data on digital media must be protected using an encryption protocol.
    1. Media is defined as any medium in which data can be stored, recorded, or printed. This includes both digital and non-digital media.
        i. Digital media is a form of content that is stored in a digital format, which can be easily accessed and manipulated using electronic devices. Examples of electronic devices include but are not limited to computers, smartphones, tablets, flash storage, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Digital media encompasses a wide range of multimedia content, including text, images, audio, video, and interactive elements, and it is often distributed through the internet and various digital communication channels.
    2. Non-digital media includes all data storage and records which are not stored within an electronic device. This includes but is not limited to paper and microfilm.
    3. Securely storing sensitive digital data includes implementing industry approved encryption protocols. All media storage devices that store sensitive data should employ a hardware-level encryption solution, such as Windows BitLocker or Linux dm-crypt. All portable media must employ an encryption methodology that requires a password, token, or other means of authentication to decrypt.

4. All devices which store sensitive information must be included in an automated or manually maintained inventory. Each agency must employ a procedure for documenting access requests and the return of both digital and non-digital storage media. Digital media storage devices should be cataloged with a make, model, and other identifying information, as well as the responsible party.
5. Media storage solutions must be appropriate for the data which it will contain. For example, backups of sensitive data should be stored via encrypted hard drives or tapes as opposed to flash drives. All media storage devices and records should be classified according to the sensitivity of the data stored within.
6. Storage media may not be subject to the above security standards if it only contains data that has been determined to be in the public domain, publicly releasable, or have limited adverse impacts if accessed by other than authorized personnel. Each agency must employ a process classifying sensitive and non-sensitive data that includes approval by key stakeholders.

B. Each agency must limit access to sensitive data on digital and non-digital media to only authorized users based on a user's need to know.
    1. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.

C. Each agency must sanitize or destroy digital and non-digital system media containing sensitive data before disposal or release for reuse.
    1. Establish a data retention policy that defines when sensitive data must be destroyed.
    2. Ensure the disposal process and method are commensurate with the data sensitivity.
    3. Examples of the types of digital media include scanners, copiers, printers, notebook computers, workstations, network components, mobile devices.
    4. Examples of the types of non-digital media include paper and microfilm.
    5. Sanitize or destroy digital and non-digital system media containing sensitive data before disposal or release for reuse.
        i. The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed.
        ii. Acceptable sanitization techniques may include clearing, purging, cryptographic erasure of digital media, de-identification of personally identifiable information, and destruction. Non-digital media should be thoroughly scrubbed to remove all sensitive data prior to release or rendered irrecoverable via cross-cut shredding or incineration. Digital media should be destroyed via methods such as low-level wiping, degaussing, or physical destruction.
    6. Ensure that all sensitive data stored and/or hosted by third parties is sanitized or destroyed. The agency should require that the third-party provide certificates of destruction or sanitization when the process is complete.
    7. Ensure that appropriate confidentiality agreements are in place for all sensitive agency data stored and/or hosted by third parties.

D. Each agency must review sensitive data and determine if the media should be marked with necessary confidentiality markings and distribution limitations.
    1. Examples of where data may not need to be marked include publicly releasable data or data that remains in secure areas controlled by the agency.

E. Each agency must control access to media containing sensitive data when outside of controlled areas via hardware-level encryption or password authentication on all digital media.
    1. All media, both digital and non-digital must be assigned to a responsible party prior to its departure from a controlled area via a documented process. This may be satisfied through a log sheet that denotes the responsible party and a timestamp of the media's departure and return or an automated inventory system.

F. Each agency must encrypt sensitive data stored on digital media.

G. Each agency must control the use of removable media on system components.
    1. Limit the use of portable storage devices to only approved devices, including devices provided by the agency, devices provided by other approved entities, and devices that are not personally owned.
    2. Portable storage devices must be restricted to functionality only necessary for their intended purpose. Devices which do not require the ability to be written to should be configured as "Read Only".
    3. Disable autorun and autoplay functionality for removable media.
    4. Configure antimalware software to automatically scan removable media.

H. Each agency must prohibit the use of portable storage devices when such devices have no identifiable owner.

I. Each agency must protect recovery/backup data with equivalent controls to the original data. This includes encryption and data separation, based on requirements.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 12: Personnel Security

Rule 12.1 Personnel Security Protection

A. Each agency must screen individuals prior to authorizing access to any non-public agency systems or data. Screening activities include but are not limited to the evaluation/assessment of an individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual).
    1. Ensure that all staff which are provided access to non-public data are subject to, at a minimum, background checks in accordance with applicable laws.

B. Each agency must ensure that access to agency systems and data are protected during and after personnel actions such as terminations and transfers.
    1. Establish a documented process for disabling user access within a predefined time upon employee departures. This may include disabling or deleting user accounts, VPN access, and the return or disablement of access tokens and

keys.
2. Consider timely execution of termination actions for individuals terminated for cause. In certain situations, agencies must consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified.
3. Ensure that all security-related agency system-related property is retrieved and retain access to all agency information and systems formerly controlled by the terminated individual.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 13: Physical Protection

Rule 13.1 Physical Protection

A. Each agency must limit physical access to agency systems, equipment, and the respective operating environments to authorized individuals. Limiting physical access requires the implementation of physical security controls to restrict an individual's ability to interface with a given device.
    1. Limiting physical access should be applied to all individuals who enter its facility or perimeter. This includes, but is not limited to staff, visitors, and other third parties which retain access credentials.
    2. Develop and maintain documented processes which describe the methods in which they restrict access and enforce physical access authorizations, to include the location of mission critical devices and systems, their applicable physical security control, and how access is delegated and removed from users.
        i. Limiting physical access to equipment may include placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only; and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.

B. Each agency must protect and monitor the physical facility and support infrastructure for agency systems. Known or observed vulnerabilities or gaps in the physical security of an organization's perimeter or facility must be addressed immediately.

C. Each agency must escort visitors and monitor and control visitor activity.
    1. Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

D. Each agency must maintain and audit logs of physical access.
    1. Audit logs can be procedural (e.g., a written log of individuals accessing the facility), automated (e.g., capturing ID provided by an access card/badge), or some combination thereof. Physical access points can include facility access points, interior access points to systems or system components requiring

supplemental access controls, or both. System components (e.g., workstations, notebook computers) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

2. ITS recommends that agencies review physical access logs monthly and upon occurrence of detected and/or suspected physical security incidents/violations.

E. Each agency must control and manage physical access devices.
   1. Physical access devices include but are not limited to keys, locks, combinations, biometric readers, and card readers. These devices must be secured when not in use.
   2. Document the location in which access devices and keys are stored as well as individuals which are granted access to them.
   3. Inventory physical access devices at least annually.
   4. Change physical access devices (e.g., combinations and keys) *at minimum* yearly and/or when keys are lost, combinations compromised, or when individuals possessing the keys or combinations retire, leave, and/or are transferred or terminated and/or access is no longer needed.

F. Each agency must ensure protections for agency systems are in place for alternate work sites.
   1. Alternate work sites may include government facilities or the private residences of employees.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 14: Risk Assessment

Rule 14.1 Risk Assessments

A. Each agency must periodically assess the risk to agency operations resulting from the operation of agency systems and the associated processing, storage, or transmission of data.

B. Each agency must conduct a risk assessment that considers threats, vulnerabilities, likelihood, and impact to agency operations and assets, individuals, other organizations, and state government.
   1. Identify threats and vulnerabilities to agency systems.
      i. An inventory of all hardware, software, and user access must be established and maintained as an agency experiences any substantive change. Please refer to Part 1, Chapter 2, 2.1 System and Physical Device Inventory.
   2. Identify threats and vulnerabilities from third parties, including, but not limited to, third parties who operate systems on behalf of the agency and/or process, store, or transmit information on behalf of the agency.
      i. Identify all third parties which provide functionality to the organization via either hardware or software. Agencies will inventory and document the data and network resource access that all third parties are provided access.

ii. Determine the sensitivity of data that each third party is provided access to and incorporate said access into its risk assessment.
iii. Define the legal and regulatory standards that the data accessible to the third party is subject to and establish contracts or other Service Level Agreements to describe the ability and expectation of the vendor to satisfy the applicable standard.
iv. Monitor and ensure (to the extent possible) that the third party meets the expectations of any agreement or contractual obligation regarding information security and/or privacy.

3. Determine the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, loss, or destruction of/to the system and/or the information it processes, stores, or transmits, and any related information.
4. Determine the likelihood and impact of adverse effects on individuals arising from the collection and/or processing of personally identifiable information (PII).
    i. ITS recommends agencies conduct privacy impact and/or privacy risk assessments to help determine the likelihood and impact of adverse effects for PII. A privacy risk and/or privacy impact assessment evaluates the risks, controls, and consequences associated with collecting, maintaining, using, and/or disclosing personally identifiable information (within and outside of the agency) so that the agency can make informed decisions regarding risk mitigation, protection of the data, and compliance with applicable legal requirements and best practices.

5. Integrate risk assessment results and risk management decisions from the agency and mission or business process perspectives with system-level risk assessments.
6. Document risk assessment results in appropriate agency security and privacy plans.
7. Respond to findings from security and privacy assessments, monitoring, and audits in accordance with agency risk tolerance and update the risk assessment as needed.
8. Review and update the risk assessment, as needed, in accordance with agency risk tolerance based on security and privacy assessments, monitoring, and audits; supply chain issues; security incidents or breaches; changes in law, executive orders, directives, regulations, policies, standards, or guidelines; and changes to and/or availability of new technologies, individuals, external parties, and assets in accordance with agency risk tolerance.

C. Each agency must perform automated vulnerability scans for vulnerabilities in agency systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
    1. Perform automated vulnerability scans of internal agency assets on a monthly, or more frequent, basis. Conduct both authenticated and unauthenticated

scans, using a SCAP-compliant vulnerability scanning tool. The agency must maintain the results of vulnerability scans for a period of at least one year.

2. Perform automated vulnerability scans of externally exposed agency assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis. The agency must maintain the results of vulnerability scans for a period of at least one year.

D. Each agency must remediate detected vulnerabilities on a monthly, or more frequent, basis, based on the remediation process.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 15: Cybersecurity Assessments

Rule 15.1 Cybersecurity Assessments

A. Each agency must conduct a comprehensive cybersecurity assessment at least once every two years to evaluate the security controls in agency systems to determine if the controls are effective in their application and to identify the current security posture of its information systems and the agency. Cybersecurity assessments must also include external parties, including, but not limited to, service providers, contractors/third parties, *etc*. who operate systems on behalf of the agency and/or process, store, or transmit information on behalf of the agency.

1. Each agency must employ an ITS-approved independent, impartial third-party provider to conduct the comprehensive cybersecurity assessment. Comprehensive cybersecurity assessments must include *at minimum* the below and should be modeled from all guidelines specified in the Comprehensive Cybersecurity Assessment Guidelines document that can be found on the ITS website.
    i. Perform an assessment of the security controls in the information systems and their environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.
    ii. Incorporate results from other types of assessment activities such as vulnerability scanning and system monitoring, to maintain the security and privacy posture of systems during the system life cycle.
    iii. Perform external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit agency systems.
        a. Penetration testing must be appropriate to the size, complexity, and maturity of the agency environment. Penetration testing activities include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise control.
            1. Cloud-based services which are identified as a

component of agency business functionality must be included in Security Assessments. This includes cloud-based backup solutions, user access control platforms (e.g. Microsoft 365), file-sharing and storage platforms (e.g. SharePoint, Box), and other Content Management Systems (e.g. AWS, Akamai).

b. Penetration testing must occur from outside the agency's network perimeter (i.e., outside the agency's firewall but inside the Enterprise State Network's security border) as well as from within the agency's boundaries (i.e., on the internal agency network) to simulate both outsider and insider attacks. Penetration testing helps determine the minimum set of controls required to reduce and maintain risk at an acceptable level.
c. Control and monitor any user or system accounts that are used to simulate both outsider and insider attacks to ensure they are only being used for legitimate purposes and are removed or restored to normal function after testing is completed.
d. Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.
e. Validated vulnerabilities discovered during the penetration tests must be documented and mitigated in a timely manner.
    1. Vulnerabilities should be prioritized based on the criticality of both the vulnerability and the system/application.
f. Penetration tests should include a full scope of blended attacks, such as wireless, client-based, and web application attacks.
g. Agencies which develop in-house applications that have a defined development cycle will create a test bed that mimics a production environment for specific penetration tests attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.

iv. Perform social engineering training campaigns and simulated threats to assess the security posture and employee adherence to established security policies and practices. This may include either email phishing, voice vishing, or a combination of both attacks. Testing should not be designed to target a specific person, but rather target the corporate culture, to include all agency staff.
v. Cybersecurity assessments must include applications to ensure key security and privacy requirements are met. Code in the application and supporting infrastructure must be tested for common errors that can compromise the integrity of the production environment when the application is deployed.
    a. ITS recommends that all new applications have a

comprehensive assessment performed by a third-party prior to its release into a production environment.

vi. ITS recommends performing advanced persistent threat (APT) assessments to identify weaknesses that could be used in a targeted and/or advanced attack. The goal of an APT is to gain access, escalate privileges, and remain hidden so as to exfiltrate sensitive data. This type of assessment includes a higher level of agency reconnaissance, a more prolonged period of engagement to facilitate a deeper understanding of more complicated attack possibilities, and many times utilizes social engineering. Further, ITS recommends periodically assessing the current environment for indications of an incident such a breach.

vii. ITS recommends including tests for the presence of overly permissive network resources which are used to share data. This includes assessment of Access Control Lists and the storage of data in network shares which is identified as sensitive. This may include information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, and backups of emails or documents containing passwords or other information critical to system operation.

B. Each agency must develop and implement a plan of action and milestones to document the planned remedial actions to correct weaknesses or deficiencies and reduce or eliminate known vulnerabilities in agency systems.
    1. Update plan of action and milestones based on findings from ongoing assessments, audits or reviews, and continuous monitoring activities.

C. Each agency must submit all cybersecurity assessment reporting deliverables to ITS. Reporting requirements are included in the Cybersecurity Assessment Reporting Guidelines which can be found on the ITS website. All reporting deliverables from the cybersecurity assessment must be submitted within 90 days of its completion.

D. Each agency must monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
    1. Continuous monitoring efforts facilitate ongoing awareness of threats, vulnerabilities, and information security to support agency risk management decisions.
    2. Additional cybersecurity assessments should be performed when there are significant changes to information systems and their environment of operation, new threats and vulnerabilities are identified, or other conditions occur that may impact the security state of the system or its environment.

E. Each agency must develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 16: System and Communication Protection

Rule 16.1 System and Communications Protection

A. Each agency must monitor, control, and protect communications (i.e., information transmitted or received by agency systems) at the external boundaries and key internal boundaries of agency systems.
    1. Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).
        i. ITS recommends not using WPA2 Personal (standard wireless network keys) as opposed to WPA2 Enterprise (username and password wireless authentication).
    2. Perform traffic filtering between network segments, where appropriate.
    3. Collect and store all network traffic flow logs and/or network traffic in a centralized server. All traffic logs must be retained for a predetermined period defined by the agency. Logs shall be reviewed at consistent intervals, or in response to a perceived or realized security event.

B. Each agency which develops in-house software must employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
    1. Establish and maintain a secure network architecture. A secure network architecture must address the following, at a minimum:
        i. Network segmentation: Development and production environments should be separated logically from one another. Further, network segmentation should exist between areas of differing data sensitivity levels.
        ii. Least privilege: Software and systems shall be designed in a way users are only afforded permissions to necessary functionality and information.
        iii. Availability: Software shall be designed in a manner that does not negatively impact the availability of other agency resources.
    2. Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

C. Each agency must separate user functionality from system management functionality.
    1. Agencies can implement separation of system management functionality from user functionality by using:
        i. Different computers, different instances of operating systems, or different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate.
        ii. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other system resources.

iii. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

2. Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the agency's primary network and not be allowed internet access.

D. Each agency must prevent unauthorized and unintended information transfer via shared system resources. It is recommended that only Common Criteria (CC) approved systems (such as Windows, Apple, Linux) are used. The CC evaluated systems have been certified to protect against misuse of shared resources.

E. Each agency must implement DMZ subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

F. Each agency must deny network inbound communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

1. Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. The agency should reassess this bi-annually, or more frequently.
2. ITS recommends deploying port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

G. Each agency must prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

H. Each agency must implement cryptographic mechanisms to prevent unauthorized disclosure of sensitive information during transmission unless otherwise protected by alternative physical safeguards.

1. Encrypt sensitive data in transit. Example implementations can include Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

I. Each agency must terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. For example, this includes inactivity timeouts on management sessions to network devices and servers in addition to inactivity timeouts on user network sessions such as VPN connections and other network sessions.

J. Each agency must establish and manage cryptographic keys for cryptography employed in organizational systems. For example, agencies should determine what cryptographic keys (TLS certificates, VPN keys, *etc*.) are in use. Document how these keys are managed and protected.

K. Each agency must employ federal information processing standards (FIPS)-validated cryptography when used to protect the confidentiality of sensitive information.

L. Each agency must prohibit remote activation of collaborative computing devices such as microphones, webcams, and screensharing applications. Users must be prompted with an indication that these devices are "in use" after activation.

M. Each agency must control and monitor the use of mobile code.
    1. Mobile code includes software programs or part of a program obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient. Mobile code technologies include, but are not limited to Java, JavaScript, ActiveX, Postscript, PDF, VBScript.

N. Each agency must control and monitor the use of Voice over Internet Protocol (VoIP) technologies. This includes delegation of access to administrative and end users, monitoring traffic flows, and review of any logging and alerts.

O. Each agency must protect the authenticity of communications sessions. This requires authentication and encryption of traffic using FIPS-approved algorithms.

P. Each agency must protect the confidentiality of sensitive data at rest.
    1. Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

Source: Miss. Code Ann. § 25-53-201.

Part 1 Chapter 17: System and Information Integrity

Rule 17.1 System and Information Integrity

A. Each agency must identify, report, and correct system flaws in a timely manner.

B. Each agency must monitor, control, and protect communications.
    1. Establish and maintain a documented vulnerability management and remediation process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    2. Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent basis, based on the remediation process.

C. Each agency must provide protection from malware at designated locations within organizational systems.
    1. Deploy and maintain anti-malware software on all enterprise assets, where appropriate and/or supported. Further, agencies should deploy anti-malware scanning at the network level to include, at a minimum, the network external boundary.

D. Each agency must monitor system security alerts and advisories and take action in response.

1. Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

E. Each agency must update malware protection mechanisms when new releases are available.
    1. Configure automatic updates for anti-malware signature files on all enterprise assets.

F. Each agency must perform periodic scans of organizational systems on a weekly basis *at minimum*, and real-time scans of files from external sources as files are downloaded, opened, or executed.
    1. Configure anti-malware software to automatically scan removable media.

G. Each agency must monitor agency systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
    1. Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
    2. Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.

H. Each agency must identify unauthorized use of agency systems via aggregating user logins and other system events and reviewing them on a consistent basis or immediately upon identifying a potential or realized security event.

Source: Miss. Code Ann. § 25-53-201.