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: General Security Policy

Rule 1.1 Authority. This document formally promulgates the State of Mississippi Enterprise Security Policy. For the purposes of this policy, security is defined as protection of the integrity, availability, and confidentiality of information; and the protection of Information Technology (IT) assets from unauthorized use, modification, damage, or destruction. It includes the security of primary and off-site IT facilities, data storage, and operations activities; computing, telecommunications, and applications-related services obtained from other government entities or commercial concerns; and Internet-related applications and connectivity.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.2 Scope. This policy applies to all Mississippi executive and judicial branch agencies and educational institutions (hereafter referred to collectively as "agencies"), as provided by law, that operate, manage, or use IT services or equipment to support critical state business and educational functions. Where conflicts exist between this policy and an agency's policy, the more restrictive policy will take precedence. This policy encompasses systems, automated and manual for which the agencies have administrative responsibility, including systems managed or hosted by third parties on behalf of the agencies. It addresses information, regardless of the form or format, which is created or used in support of business activities for the agencies. This policy applies to all users of agency information technology resources, including all agency employees, sub-contractors, temporary workers, and vendors.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.3 Purpose. The purpose of this policy is to define a set of 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 plans, policies, and procedures. The primary objectives of this policy are to:

A. Manage the risk of security exposure or compromise by focusing on the creation of a shared and trusted environment, with particular attention to:
    1. Common approaches to end-user authentication;
    2. Consistent and adequate network, server, and data management;
    3. Appropriate uses of secure network connections;
    4. Prevent unauthorized use or reproduction of copyrighted material by public entities; and
    5. Closing unauthorized pathways into the network and into the data pursuant to Mississippi Code Annotated § 25-53-5.

B. Establish an enterprise approach to security in state government that:
    1. Promotes an enterprise view among separate agencies;
    2. Requires adherence to a common security architecture and its related procedures;
    3. Recognizes an interdependent relationship among agencies, such that strengthening security for one strengthens all and, conversely, weakening one weakens all; and
    4. Assumes mutual distrust until proven friendly, including relationships with government, trading partners, and anonymous users to ensure secure interactions.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.4 Agency Directives. Each agency will establish a framework to initiate and control the implementation of security policies and standards within the agency. The head of each agency will ensure that an organization structure is in place for:

A. Operating in a manner consistent with the ITS Enterprise Security Policy;
B. Developing, implementing, maintaining, and complying with its own security plan and security policy;
C. Developing, implementing, maintaining, and testing security processes, procedures, and practices to protect and safeguard voice, video, and data computing and telecommunications facilities—including telephones, hardware, software, and personnel—against security breaches;
D. Training and educating all agency employees, associates, business partners, and others using its computers or networks to follow proper IT security procedures and standards;
E. Applying appropriate security measures when developing applications;
F. Implementing a security awareness program; and
G. Ensuring and overseeing compliance with this policy.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.5 ITS Security Officer; Role and Responsibilities. ITS has designated a Chief Information Security Officer (CISO) that is responsible for developing and maintaining the State of Mississippi Enterprise Security Policy. The ITS CISO and his staff will be responsible for:

A. Developing and maintaining the State of Mississippi Enterprise Security Policy.
B. Researching the IT industry for security related issues and determining how they affect the state IT infrastructure as a whole.
C. Participating in local and national security organizations for the purpose of sharing security information and developing best practice policy and procedure.
D. Working with state agencies on all security related issues.
E. Maintaining a state security listserve for the purpose of distributing security advisories and facilitating security discussion among the agency security contacts.
F. Maintaining a state security website for the purpose of sharing information, accessing contracts and documents, distributing security advisories, incident reporting, and education and awareness opportunities.
G. Working with agencies, technical support staff, and law enforcement where necessary, in the investigation of security incidents, intrusion attempts, and virus attacks. Reporting to agencies on these intrusion attempts and virus attacks.
H. Working with State Auditor's Office on IS audits as necessary.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.6 Agency Security Officer Roles and Responsibilities. ITS requires that each agency designate an individual as their agency's Security Officer. For agencies with small IT infrastructures, this designation could be a shared duty assumed by an existing member of the agency staff. For other agencies with very large/complex IT infrastructures, this designation requires that security be a major duty/responsibility for that individual. The agency Security Officer will be responsible for:

A. Developing and maintaining agency-specific security plans, policies, and procedures.
B. Interacting with ITS as the primary contact for security related issues.
C. Ensuring that their agency is adhering to the State of Mississippi Enterprise Security Policy.
D. Participating in the state information security listserve.
E. Researching IT industry for security related issues and how it affects their agency specifically.
F. Monitoring security issues within the agency's IT resources.
G. Facilitating the State Auditor's Information Systems Audit and the Third Party Risk Assessment.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.7 Auditing and Compliance; State Auditor's Role. Compliance with security policies is the responsibility of all state agencies. Any agency that fails to comply with security policies endangers everyone else in state government. Thus the following policy is established to clarify the role of the State Auditor and the Department of Information Technology Services, Information Security Division in auditing compliance:

A. The State Auditor will review how well agencies comply with security policies as part of their normal agency information systems auditing activities.
B. As a component of their standard Information Systems audit process, the State Auditor will consider the Enterprise Security Policy in the review of the systems, processes, and procedures that they will examine.
C. The State Auditor may request the assistance of the ITS Information Security Division in the performance of this normal audit function.
D. 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.
E. Upon determination of any non-compliance, the State Auditor may instruct the agency and/or the ITS Information Security Division to take necessary steps to become compliant.
F. Agencies should understand that failure to comply with the Enterprise Security Policy could result in a finding in the agency's audit report from the State Auditor.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.8 State, Federal, and Industry Guidelines. Based on its individual business needs and specific legal requirements, agencies may exceed the security requirements in this policy, but must, at minimum, achieve the security levels required by this policy. It is the responsibility of each agency to determine whether there are any guidelines or regulations outside the State of Mississippi Enterprise Security Policy they are required to meet. These guidelines may include:

A. Health Insurance Portability and Accountability Act (HIPAA) http://www.dhhs.gov/ocr/hipaa/
B. Federal Privacy Act http://www.justice.gov/opcl/privacyact1974.htm
C. Federal Educational Rights and Privacy Act (FERPA) http://www.ed.govpolicy/gen/guid/fpco/ferpa/index.html
D. PCI/DSS https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
E. Tax Information Security Guidelines for Federal, State and Local Agencies http://www.irs.gov/pub/irs-pdf/p1075.pdf
F. House Bill 583 of 2010: Breach of Security; Require notice http://billstatus.ls.state.ms.us/2010/pdf/history/HB/HB0583.xml

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.9 Security Policy Exemptions. This policy applies to Institutions of Higher Education except, pursuant to section § 25-53-25 of the Mississippi Code Annotated, when they develop security policies in lieu of the ITS Enterprise Security Policy that are:

A. Appropriate to their respective environments, and
B. Consistent with the intent of the ITS Enterprise Security Policy. Such higher education security policies must address:
    1. Appropriate levels of security and integrity for data exchange and business transactions;
    2. Effective authentication processes, security architectures(s), and trust fabric(s); and,
    3. Compliance, testing and audit provisions.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.10 Maintenance of Enterprise Security Policies, Standards, Guidelines and Recommendations. The revision date for this Enterprise Security Policy is October 1, 2013. Technological advances and changes in the business requirements of state agencies will necessitate periodic revisions to enterprise security policies, standards, guidelines and recommendations. ITS is responsible for routine maintenance of these to keep them current.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.11 General Policy Requirements.

A. Each agency must operate in a manner consistent with the maintenance of a shared, trusted environment within state government for the protection of sensitive data and business transactions. Agencies may establish certain autonomous applications, including those hosted by an Applications Service Provider or other third party, outside of the shared, trusted environment, provided the establishment and operation of such applications follows all guidelines as set forth in this security policy and does not jeopardize the enterprise security environment, specifically:
    1. The security protocols (including means of secure transport, authentication, and authorization) relied upon by others; and
    2. The integrity, reliability and predictability of the state network infrastructure

B. Each agency must establish its secure state business applications within the criteria outlined in the ITS Enterprise Security Policy. This requires that all parties interact with agencies through a common security architecture and authentication process. ITS shall maintain and operate the shared state government network infrastructure necessary to support applications and data within a trusted environment.
C. Each agency that operates its applications and networks within the state government network infrastructure must subscribe to the following principles of shared security:
    1. Agencies shall follow security standards established for selecting appropriate assurance levels for specific application or data access and implement the protections and controls specified by the appropriate assurance levels;

2. Agencies shall recognize and support the state's standard means of authenticating external parties needing access to sensitive information and applications;
3. Agencies shall follow security standards established for securing servers and data associated with their applications; and
4. Agencies shall follow security standards established for creating secure sessions for application access.

D. Each agency must address the effect of using the Internet to conduct transactions for state business with other public entities, citizens, and businesses. Plans for Internet-based applications must be prepared and incorporated into the agency's security plan and submitted for review.
E. Each agency must review its IT security processes, procedures, and practices at least annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment. Examples of these changes include modifications to physical facility, computer hardware or software, telecommunications hardware or software, telecommunications networks, application systems, organization, or budget. Practices will include appropriate mechanisms for receiving, documenting, and responding to security issues identified internally or by third parties.
F. Each agency must develop, implement, and maintain their individual agency IT security policy. Each agency will annually review, and revise (as needed) its security policy. 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.
G. Each agency must develop, implement, and maintain their individual agency IT security plan. Each agency will annually review, revise (as needed), and formally transmit its security plan to ITS.
    1. Technological advances and changes in the business requirements will necessitate periodic revisions; therefore, agencies must review and update IT security plans at least annually and following any significant change to its business, computing, or telecommunications environment.
    2. If an agency purchases IT services from another entity, the agency and the provider must work together to make certain the IT security plan for the provider fits within the agency's plan. If two or more agencies participate with each other in operating an information service facility, then the agencies must provide details within their individual agency security plans regarding these projects and ensure that their plans meets their mutual needs.
    3. A portion of each agency's plan must promote security awareness by informing employees, associates, business partners, and others using its computers or networks about: security policies and practices, expectations of the users, and data handling procedures.

H. Agency heads are responsible for the oversight of their respective agency's IT security and will be required to confirm in writing that the agency is in compliance with this policy. The annual security verification letter must be submitted with the agency's security plan. The verification indicates review and acceptance of agency security processes, procedures, and practices as well as any updates to them since the last approval.

I. Each agency must obtain an IT security risk assessment from third-party security consultants at least once every three years. The agency will be required to submit a copy of the Executive Summary from the third party's assessment report to the ITS Information Security Division along with a copy of the agency's remediation plan for addressing issues identified within the assessment. Should critical or high-level risk be identified in the agency's report, the agency may be required to provide additional detailed information from the third party's full assessment report. Please be advised that any reports and/or documents resulting from a security risk assessment are classified as confidential and are not to be made available for public disclosure in accordance with Section 25-61-9 of the Mississippi code annotated. ITS recommends that agencies perform regular security assessments on their network throughout this three-year period, but it is not mandatory that they provide reporting for the additional security assessments.

J. Each agency may be subject to an Information Systems (IS) audit conducted by the State Auditor's Office. As part of the standard IS audit process, they will consider the Enterprise Security Policy as they review systems, processes, and procedures. The State Auditor may determine a special audit of an agency's IS 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 significant deficiencies revealed by the review or audit. To the extent that the audit documentation includes valuable formulate, designs, drawings, computer source codes, 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.

K. Each agency must ensure staff is appropriately trained in IT security policy, plans, and procedures. Each agency must make staff aware of the need for IT security and train them to perform the security procedures for which they are responsible. Agencies must participate in appropriate security alert response organizations at the state, regional, and national levels as required by their mission. At minimum, the agency must participate in the state's SecureNet listserve to receive security alert notifications.

L. The only permitted exceptions to the IT security policy of the State of Mississippi are those that are approved in writing by ITS for an agency's specific purpose and are only applicable to that agency's operations.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 2: State Network Resource Usage

Rule 2.1 Guest/public users must not be permitted access to the state network resources.

A. Any agency wishing to provide Internet access to a guest user must utilize one of the following approved methods:
    1. Installing separate equipment and a separate circuit for guest users. Contact ITS for more information on this method of connectivity.
    2. Tunneling guest user traffic to an ITS DMZ via the Cisco controller solution implemented by ITS. Contact ITS for more information on this method of connectivity.
B. Both methods require:
    1. No ports opened inbound to guest users.
    2. All guest user traffic must be filtered.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 2.2 Applications that pose a risk to the security of the State Network will not be permitted, including file transfer within Internet chat and peer to peer (P2P) file sharing programs.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 2.3 Each agency should consider developing an acceptable use policy (AUP) that defines the proper use of state resources by agency users. The AUP can protect users, partners, and agencies from illegal or damaging actions by individuals, either knowingly or unknowingly. Improper use of state resources exposes agencies to risks including virus attacks, compromise of state resources, and legal issues. ITS has developed an AUP for its users and it can be viewed at: http://www.its.ms.gov/Policies/Documents/itsusepolicy.pdf

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 2.4 Each agency must develop a policy that defines the use of personal devices (i.e. mobile devices, minis, laptops, personal computers) on state systems. At minimum, this policy must require those devices to be subject to the same security requirements as state owned devices. It is recommended that the agency personal device policy include information describing how personal devices may be monitored and agency expectations regarding user cooperation in the investigation of a security breach, related to state information, where the personal device is a potential source for the breach. Additionally, it is recommended that the agency require the user to sign a letter or agreement acknowledging that they agree and understand the agency personal device policy

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 3: Incident Reporting

Rule 3.1 Each agency must report all information security incidents to the ITS Information Security Division (ISD) as soon as possible.

Information security incidents result from a validation of an information security event. Information security events are defined as any violation of computer security policies, network integrity, data confidentiality, or standard computer security practices.

Detailed reporting procedures and a description of reportable events are provided in the ISD Cyber Security Incident Reporting Guidelines document. State employees can access this document from the ITS website.

A. Each agency must establish security event/incident response procedures that define the actions to be taken when a security event/incident occurs.
B. Each agency is responsible for assessing the significance of a security incident within their organization and for providing this information to ISD based on the business impact on affected resources and the current and potential technical effect of the incident (e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of sensitive information, or propagation to other networks).
C. Each agency must implement a policy requiring all agency users to report suspected security events/incidents to an appropriate level supervisor, manager, or security officer within their agency. Each agency must train their users on the procedures for reporting a suspected security event, security policy violation, state or federal law violation, theft, damage, or action placing state resources at risk.
D. Each agency is responsible for contacting the appropriate law enforcement and investigative authorities if criminal action is suspected.

Source: *Miss. Code Ann. § 25-53-1 to § 25-53-25.*

Part 1 Chapter 4: Data Classification

Rule 4.1 Data must be properly managed from its creation, through authorized use, to proper disposal. This data classification policy provides a high-level guideline to state agencies for the purpose of understanding and managing data and information assets with regard to the level of protection required. This policy requires that all data be classified on an ongoing basis and managed based on its confidentiality, integrity, and availability characteristics.

A. Each agency must establish a data classification policy and shall serve as a classification authority for the data and information that it collects or maintains in satisfaction of its mission.
    1. Data classifications are a prerequisite to establishing agency guidelines and system requirements for the secure generation, collection, access, storage, maintenance, transmission, archiving, and disposal of state data.

    2. The data classification identifies how sensitive the data is with regard to unauthorized disclosure. Data should be assigned one of three classifications:

a. ***Public:*** The "public" classification includes information that must be released under Mississippi open records law or instances where an agency unconditionally waives an exception to the open records law.
b. ***Limited Access:*** The "limited-access" classification applies to information that an agency may release if it chooses to waive an exception to the open records law and places conditions or limitations on such a release.
c. ***Sensitive:*** The "sensitive" classification applies to information, the release of which is prohibited by state or federal law. This classification also applies to records that an agency has discretion to release under open records law exceptions but has chosen to treat as highly confidential.

3. In addition to the data classification, all data must also have a designated data owner. The data owner will be responsible for assigning data classification regarding their data.

B. State and federal law may require that certain types of data be classified in a particular manner. Each agency shall determine if there are state or federal legal requirements for classifying the data and shall assign the classification(s) as required by law. (i.e. HIPAA, PCI, etc.)
C. Each agency must establish a process to regularly review the appropriateness of the assigned data classifications and adjust classifications in the event of regulatory changes affecting an agency's management of information under its control.
D. Each agency must ensure that data compiled from multiple sources is classified with at least the most secure classification level of any individually classified data in the set.
E. Each agency must ensure that data shared with other agencies is consistently classified and protected in accordance with a documented agreement detailing, at a minimum, data treatment requirements.
F. Each agency must ensure that sensitive data is secured in accordance with applicable agency requirements, federal or state regulations/guidelines, and the enterprise security policy.
G. All reproductions of data in its entirety must carry the same data classification as the original. Partial reproductions of data need to be evaluated to determine if new classifications are warranted.
H. If an agency is unable to determine the data classification of data, the data should be assumed to have high classification requirements and, therefore, is subject to a data classification of "sensitive".
I. All personally identifiable information (PII) must be classified as "sensitive".

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 5: Servers

Rule 5.1 Each agency is required to "harden" their servers. Hardening these servers includes:

A. Regularly installing all service packs, patches, and updates after appropriate integration testing.
B. Disabling all unnecessary services, devices, and accounts.
C. Enabling appropriate logging and routine log activity review procedures.
D. Establishing adequate access and control mechanisms.
E. Ensuring user authentication and data protection.
F. Performing routine scans for vulnerabilities and configuration weaknesses.
G. Setting security parameters and file protections.
H. Enabling firewall software on the server.
I. Maintaining virus scanning software on all servers.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 5.2 Proper physical location of the server must be considered. Refer to chapter 12 of the ESP for more information about physical access.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 5.3 Internet-facing servers that reside on the State Network must be properly secured to preserve the integrity of the network. Inbound connections from the Internet or any third party network will be made using HTTP or HTTPS through enterprise reverse proxy devices in the ITS DMZ.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 6: Email

Rule 6.1 To increase security and limit spam and emailed viruses, ITS has implemented and maintains mail relays on the inside and outside of the firewall. All mail bound for state domain email addresses must come through the outside mail relay and be "relayed" to the inside mail relays. The inside mail relay forwards the mail on to the appropriate mail server. All outbound mail going out passes through the inside mail relay before being forwarded to the Internet. For this reason, agencies must adhere to the following guidelines for mail:

A. No direct SMTP to and/or from the Internet. Agencies must utilize the ITS maintained mail relays for mail traveling in both directions.
B. No POP or IMAP from Internet to mail servers inside state network. Agencies must utilize a secure web interface (HTTPS) to access mail.
C. No POP or IMAP from state network to private mail accounts on Internet. Agencies must utilize a web interface (HTTP/HTTPS) to access this mail.
D. ITS recommends that Agencies forward all mail through to the inside mail relay and restrict TCP 25 inbound and outbound in their firewalls to the relays' addresses.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 6.2 Each agency must establish policies to help employees use email properly, to reduce the risk of intentional or inadvertent misuse, and to ensure that official records transferred via electronic mail are properly handled. Principle priorities include the following:

A. Email communications must not be unethical, fraudulent, harassing, obscene, or be perceived as a conflict of interest.
B. User must be instructed of the risk of opening file attachments they were not expecting to receive.
C. Email must be used to conduct official business only.
D. Clear text emails must not contain sensitive information. If sensitive information must be communicated using email, the email must be encrypted both in transport and at rest.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 7: Virus Prevention

Rule 7.1 Agencies are required to have a virus prevention program that includes:

A. Maintaining virus scanning software on all servers and workstations.
B. Keeping virus signature files and scanning engines updated on a schedule relevant to the system. Workstations must be updated at least weekly, and servers must be updated at least daily. A more stringent schedule may be adopted if the agency deems the machine a higher risk.
C. Scanning all file attachments sent or received via e-mail using current anti-virus software.
D. Scanning all removable media upon connection/ insertion using current anti-virus software.
E. Immediately removing any infected workstation or server from the network until the virus has been cleaned.
F. Maintaining copies of virus-detection tools offline.
G. Keeping all servers and workstations current with operating system and software security patches.
H. Disabling AutoPlay on all workstations and laptops.
I. Reporting all virus activity that is not automatically cleaned by the virus protection software to ISD as a security incident. Refer to Chapter 3 of the ESP for details regarding incident reporting.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 7.2 ITS will monitor for network activity that indicates the presence of malicious code and upon detection will perform the following actions:

A. For isolated infections, ITS will block access to the state network for infected workstations or servers and notify the agency contact. Once the agency contact confirms that the workstation or server has been cleaned, ITS will remove the block. Detailed information regarding this process is provided in the ISD-Ticket

Response Guidelines document. State employees can access this document from the ITS website.

B. For cases of infection within an agency that have the potential to impact other agencies, ITS will limit or remove connections to the state network for the infected agency. Such drastic action will be considered any time the availability, reliability, or integrity of the state network is at risk, but ITS will attempt to work with the infected agency to find a mitigating alternative prior to removing access.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 8: Firewalls

Rule 8.1 ITS will maintain a perimeter firewall between the State Network and the Internet. This firewall will provide address-translation to public space for state agencies.

A. Inbound connections from the Internet will be restricted to only ports TCP 80 and TCP 443, for only HTTP and HTTPS protocols. No other inbound-initiated ports will be allowed to servers residing on the State Network unless entering the state network over a VPN.
B. ITS will maintain a DMZ for applications that meet the following criteria:
    1. Require inbound connections that are not HTTP or HTTPS
    2. Declared business-critical by both the agency and ITS
    3. Deemed as unsuitable for a VPN by ITS

C. All applications utilizing the ITS DMZ must reside in the State Data Center.
D. Outbound connections from the State Network will be largely unrestricted. Exceptions to this include LAN protocols, ICMP, and ports known for propagating malicious code.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 8.2 Each agency is required to implement a firewall at the perimeter of their network, to secure the LAN from any traffic originating within the State Network. Each agency should define a rule set for their firewall that is as restrictive as possible, permitting the minimum services required for proper operation of inter-agency communication. All services not required for proper operation should be denied by the rule set.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 8.3 Firewalls must only be managed using secure protocols such as SSH or HTTPS, and management should be allowed only from selected agency workstations.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 8.4 Firewall event logging must be enabled and the logs maintained for at least 30 days.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 9: Data Encryption

Rule 9.1 ITS requires that all sensitive data be encrypted using industry standard algorithms Triple DES, AES, or SSL/TLS when traveling to/from un-trusted networks and/or entities.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 9.2 If an agency Internet-facing server gathers or transmits sensitive data, the application must use, at minimum, SSL for the transaction. The agency must acquire the Certificate Authority signed certificate for this server from ITS.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 9.3 Each agency should consider encrypting the transmission of all sensitive data.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 9.4 Each agency must encrypt sensitive data stored on any of their local systems. Agencies must also ensure that any sensitive data on systems located offsite is properly encrypted.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 10: Remote Access

Rule 10.1 The following policies address connectivity into the state network from any entity that resides outside the state network. This includes third party entities' connectivity into the state network via both the public Internet and private circuits.

A. 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.
B. 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).
    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.

C. 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. It should be understood that 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 while the tunnel is connected (as defined above) does not meet the requirements or intent of this security policy.

D. 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.

E. ITS maintains Cisco VPN termination devices to establish client-based and LAN-to-LAN VPNs for access to resources on the state network.

1. All LAN-to-LAN VPNs will be implemented using the IPSec protocol.
2. Any third party entity that needs an inbound connection to the state network must provide and maintain a compatible industry-standard IPSec-capable VPN hardware/software solution at their end of the connection. VPNs must be addressed using public IP addresses registered to that entity, including the peer address and any networks at the third party that will be encrypted by the tunnel. The ITS side of the connection will adhere to the same requirements, but with the public IP addresses provided by ITS.
3. Client-based VPNs may be implemented with IPSec or SSL.

F. At no time may an agency permit a third party entity to connect directly to their local area network behind the state's border firewall and/or the agency's firewall. This includes terminating third party circuits behind ITS and agency firewalls and/or utilizing a PC remote control product (unless approved in writing by ITS) via a dialup or Internet connection. This does not include remote support applications that require real-time interaction by the agency end user, such as GoToAssist and WebEx.

G. If an agency provides dial-in access to agency personnel either via a remote access service or PC modem on their LAN or via an outsourced remote access service, the agency must implement a firewall to control access to and from the local area network by the dial users. The agency will be held responsible for any dial user that uses their facilities to access and manipulate or abuse any other facility.

H. It is essential that all access to the state's network be terminated immediately upon the retirement, resignation, dismissal, end of contract, or any and all other actions that signal that the requirements for having a connection are no longer being met.

I. At no time should any employee, vendor or account holder provide their login, user information or password to anyone. Employees, vendors or account holders are assigned individual accounts that must never be treated as a shared account.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 11: Passwords

Rule 11.1 ITS requires, at minimum, that each state agency utilize the following guidelines when developing their password policy. Each agency must enforce their developed password policy and educate their users on the choice and protection of passwords.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 11.2 Each agency must adopt the following guidelines for password administration:

A. Automated password input must not be allowed, except for simplified/single sign on systems that have been approved by ITS
B. Passwords must not be stored in clear text on hard drives or any other electronic media. If stored on electronic media, passwords must be classified as sensitive. Refer to Chapter 9 of the ESP for details regarding data encryption.
C. Access to password-protected systems must be timed out after an inactivity period of thirty (30) minutes or less.
D. Passwords for administrative accounts and accounts with access to sensitive data must be treated with a higher level of security, including:
    1. Requiring password changes every thirty (30) days
    2. Consideration of two-factor authentication

E. Third-party support accounts must be disabled or deleted when not in use.
F. Immediately revoke access when an account owner leaves or is terminated.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 11.3 Each agency must enforce the following guidelines for user password creation:

A. Passwords must contain at least 8 characters.
B. Passwords must contain a combination of lower case letters, upper case letters, numbers, and at least one symbol.
C. Passwords must not contain the user ID.
D. Passwords must not include personal information about the user that can be easily guessed: user's name, spouse's name, kid's name, employee number, social security number, birth date, telephone number, city, etc.
E. Passwords must not include words from an English dictionary or foreign-language dictionary.
F. Passwords must not contain proper names, including the name of any fictional character or place.
G. Passwords must not contain any simple pattern of letters or numbers such a "qwertyxx", "12345678", or "xyz123xx."
H. Passwords must not be trivial, predictable or obvious.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 11.4 Each agency must instruct their users to follow these guidelines for the purpose of protecting passwords:

A. Passwords must not be disclosed to anyone except in emergency circumstances or when there is an overriding operational necessity.
B. Hard copies of passwords (i.e. printed out or written down) should be considered sensitive.
C. Passwords must not be sent in clear text over the network. Secure Shell (SSH) and HTTPS must replace Telnet and HTTP for authentication.
D. Passwords must be unique per user.
E. The password change interval is a maximum of ninety (90) days; however, ITS recommends that agencies consider using a 30 or 60 day interval depending on the classification of their data. Password reuse should be minimized or prohibited.
F. Default passwords must be changed.
G. Passwords must be required on all user accounts.
H. Passwords suspected to be stolen or cracked must be changed immediately and notification must be given to the user's supervisor and system administrator.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 11.5 For users that have access to sensitive data or that have system administrator rights, agencies must consider using two-factor authentication. Two-factor authentication is a system wherein two different factors are used in conjunction to authenticate.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 12: Physical Access

Rule 12.1 All data center facilities must be physically protected in proportion to the criticality of the business functions and associated systems, assets, and infrastructure.

A. Any computing resource connected to an agency LAN or to the State Network must be placed in an area that can be locked. Any PC that is left unattended during the day must be logged out or locked when inactive. Refer to Chapter 11 of the ESP for details regarding password requirements.
B. At minimum, wiring closets must be kept in an area that can be locked.
C. At minimum, State Network routers or switches must be kept in an area that can be locked. This includes remote offices.
D. Agencies should ensure that all laptops are stored in secure locations.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 12.2 Agencies with larger computer installations must:

A. Protect access with an access control system, normally a card access system.
B. Establish procedures for granting, modifying, and revoking access.
C. Establish procedures for recording information (date, time, etc.) to track access.
D. Require security related clearance as a result of employment. (For example, all ITS employees that have access to State Data Center facilities are sworn in as Information

Confidentiality Officers as defined by legislation and are subject to background checks).

E. Use cameras to record activity in and around computer installation.
F. Establish a policy for archiving access system and video data. Agencies must archive access system and video data for a minimum period of 30 days.
G. Restrict visitors in the computer facilities. Visitors that are allowed access must sign a sign-in/out log and must be accompanied by an authorized staff member.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 12.3. Agencies with smaller computer installations must:

A. Protect access with locked rooms, at minimum.
B. Establish procedures for granting, modifying, and revoking access.
C. Establish procedures for recording information (date, time, etc.) to track access.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 12.4 Agencies should adhere to the following miscellaneous physical security guidelines:

A. Each agency should locate alternate space that meets the same physical security requirements for a business recovery site. This site should be accessible 24/7/365.
B. Backup and recovery materials (tapes, manuals, etc.) must be kept at a site that meets all security measures defined in this document. This site should be accessible 24/7/365.
C. Areas housing environmental or electrical systems critical to computer facilities should be in a location that meets all security measures defined in this document.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 13: Wireless Access

Rule 13.1 The following policies address security and data integrity measures required for implementing and securing wireless local area networks that reside within the state network.

A. Any unauthorized and/or neglectful installations of wireless networks that expose the state's network infrastructure to intruders and/or attacks may result in that agency's connection to the state network being isolated.
B. Maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems.
C. Agencies must assess risks more frequently and test and evaluate system security controls more frequently when wireless technologies are deployed.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 13.2 At minimum, the following security standards and network configurations are required for the deployment and operation of all wireless network installations:

A. The placement of wireless LAN Access Points (WAP) must be strategically located to minimize the interception of wireless signals by unauthorized individuals. The range

of the signal must also be tested to ensure that signals are not being transmitted outside the intended coverage area.

B. All WAP installations must use encryption. WPA Version 2 with AES is the minimal level of acceptable encryption. WEP and WPA (version 1) are not permitted.
C. WPA Version 2 may be deployed in either "PSK mode" or "Enterprise mode" with specific requirements for each mode.
    1. PSK mode deployment requirements:
        a. The "key" or "pass-phrase" should be known and kept securely by as few personnel as possible.
        b. The "key" or "pass-phrase" should be changed regularly. Regularly is defined as every three months for minimum standards, however, it is recommended to be changed every month.
        c. Very strong password creation practices should be followed when creating WPA-PSK passwords. At minimum, 16 characters with a combination of lower case letters, upper case letters, numbers, and symbols should be used.

    2. Enterprise mode deployment requirements
    Enterprise mode indicates that, in addition to encryption keys on the WLAN, user credentials are required for access. This mode is recommended as more secure than PSK mode, due to the second factor being required. Two known methods for implementing enterprise mode are:
        a. Radius server with rolling PSK.
        b. Manual change of PSK as described in PSK mode, with network access control deployed.

D. All WAP configuration parameters (Service Set Identifier (SSID), keys, passwords, channels, etc) that can be changed from the default manufacturer settings must be changed from the default.
E. WAPs must be connected to a switch and not a hub.
F. Physical security of WAPs must be maintained to protect the WAP from theft or access to the data port.
G. Open broadcasting of the SSID must be disabled.
H. Wireless encryption protocols only secure the LAN radio transmissions. Any sensitive data must still be handled with the appropriate network-transmission protocols. Refer to Chapter 9 of the ESP for details regarding data encryption. Each agency should consider the use of VPNs for specific users or network segments that need to transmit sensitive data.
I. Software and firmware updates from the wireless manufacturer should be applied to the WAP and affected wireless cards as soon as possible after release.
J. Additionally, the following wireless security best practices are recommended for deployment and operation of a wireless network.
    1. All WAP installations should be inventoried and the area in which the wireless LAN is installed should be regularly inspected for unauthorized WAPs or other devices not part of the approved installation. The network

should be regularly inspected both physically and electronically using sniffing tools to uncover rogue WAPs and devices.
2. The network should be scanned on a regular basis to detect unauthorized clients.
3. Agencies with large, complex scale wireless implementations should consider using a solution that provides for centralized configuration and management of the wireless access point rather than individually maintaining each WAP.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 14: Laptop and Mobile Device Usage

Rule 14.1 Each agency must adhere to the following policies for mobile devices with sensitive data. A mobile device is defined as any electric and/or battery operated device that can be easily transported and that has the capability for storing, processing, and/or transmitting data including Laptops, Portable Digital Assistants (PDAs), Tablet/Mini PCs, Blackberries, SmartPhones, and Hand-Held PCs. It is recommended that agencies consider enforcing some or all of these policies for any mobile device regardless of classification of the data.

A. Agencies employing the use of mobile devices for access to agency systems or storage of agency data must appropriately secure those devices to prevent sensitive data from being lost or compromised, to reduce the risk of spreading viruses/malware, and to mitigate other forms of abuse.
B. While traveling and using a mobile device in public places, never leave the device unattended and take precautions to avoid the risk of unauthorized persons viewing information on-screen.
C. Agencies must consider software that aids in tracking and recovery of the mobile device if lost or stolen.
D. Agencies that allow the use of mobile devices for access to state data, must consider implementing a management platform that allows them to administer the appropriate security policy to all devices supported by the agency.
E. Access Control
    1. Prohibit users from downloading, running, and/or installing software and applications or enabling unauthorized protocols or services without agency IT approval and assistance.
    2. Mobile device users must minimize the potential loss of data via WiFi, 3G, or Bluetooth connections to their device by configuring them in a secure manner or turning those services off when not in use.
    3. Disable boot-up capabilities of other drives. Disabling the secondary boot drive sequence hinders the ability to access the system from a secondary drive.
    4. Rename the Administrator Account using a non-descript name.
    5. Prevent the last user name from displaying in the login dialog box.

6. When connected to the state network, ensure only one active connected network interface is enabled at a time. For example, if WiFi is enabled, then other access methods are disabled.
7. Establish hard drive and/or BIOS password standards for the agency or each department of the agency. Enable these features on each mobile device and configure a password per this standard.

F. Authentication
   1. All mobile devices must require authentication before accessing state resources/services. Where mobile devices will have access to sensitive information, the agency should consider two-factor authentication and at minimum use strong authentication/password characteristics.
   2. Mobile devices should be configured to timeout after 30 minutes of inactivity and require re-authentication. Authentications must not be disabled on the mobile device.
   3. Agencies should require users to log out or turn mobile devices off if leaving the device unattended.

G. Encryption
   1. Refer to chapter 9 of this document for information regarding data encryption.
   2. Many mobile devices support the use of removable storage devices to store data. If sensitive data is stored on removable storage devices, the data must be encrypted.
   3. Consider implementing whole disk encryption. Whole disk encryption is preferred as it "locks" the hard drive preventing it from being accessed by physically installing it in similar equipment.
   4. Consider installing disk wiping technology that remotely wipes the mobile device clean in the event of loss or theft.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 15: Disposal of Hardware/Media

Rule 15.1 Each agency must determine if hardware/media contains any sensitive data prior to disposal (scrap, destroy, transfer or rental/lease return). If hardware/media contains sensitive data, one of the following methods must be used prior to disposal.

A. Physical Destruction
   This is the primary method that should be used for the disposal of data storage devices containing sensitive data. The intent is to completely destroy the data storage device beyond any possibility of data recovery.
      1. The agency should perform a complete and permanent elimination of data on the data storage device.
      2. Physical destruction of data storage devices is performed by shredding, disintegrating, incinerating, pulverizing, and melting the data storage device

3. If a third party is contracted for the disposal of the data storage device, a certificate of destruction must be obtained.

B. Overwriting
This method should be used in cases of exception when physical destruction of data storage devices is not reasonable or is prohibitive.
    1. Agencies may sanitize magnetic media (i.e. hard disk) by an overwriting process, whereby a software utility writes a combination of characters (usually 0s and 1s) over each location on the data storage device multiple times.
    2. This process obscures the previous information, rendering the data unreadable. Agencies must overwrite the device a minimum of three times prior to disposal.
    3. To verify the overwriting process, agencies should attempt to recover the data by one or more commercially available "data recovery utilities".
    4. Simply erasing and reformatting a data storage device is not a permissible method of sanitizing a data storage device before disposal.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25*

Rule 15.2 Each agency must erase all data and configuration information, regardless of the classification of data, prior to disposal (scrap, destroy, transfer, or rental/lease return) of hardware.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25*

Part 1 Chapter 16: Application Assessment and Certification

Rule 16.1 Each agency must perform security assessments on all new applications to ensure key application 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. Agencies should use one or more of the following application security assessment methods:
    1. Contract with a third-party for assessment services
    2. Perform Internal application security assessments
    3. Utilize application security assessment software

B. At minimum, the following vulnerabilities must be assessed.
    1. Un-validated input
    2. Broken access control
    3. Broken authentication and session management
    4. Injection flaws
    5. Improper error handling

6. Insecure configuration management
7. Insecure storage
8. Cross-Site scripting (XSS)
9. Insecure direct object references
10. Cross-Site request forgery (CSRF)
11. Insufficient transport layer protection
12. Unvalidated redirects and forwards

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25*

Rule 16.2 Each agency must document their application security assessment process/results prior to deploying new applications. Agencies must include all application assessment documentation to ITS as part of the submission package satisfying the mandatory third-party security risk assessment. Refer to Chapter 1 of the ESP for details regarding security risk assessments.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25*

Rule 16.3 Application security assessments must performed when an application is modified or updated. ITS recommends that agencies perform application assessments on a regular basis.

A. Follow-up application security assessment documentation must be submitted to ITS as part of the submission package satisfying the mandatory third-party security risk assessment. Refer to Chapter 1 of the ESP for details regarding security risk assessments.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25*

Part 1 Chapter 17: Removable Media

Rule 17.1 Agencies must adhere to the following policies for removable media regardless of classification of the data being stored.

A. Removable Media is defined as a device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This removable media policy pertains to, but is not limited to all devices and accompanying media that fit the following criteria:
    1. Portable USB-based flash drives, also known as thumb drives, jump drives, or key drives;
    2. Memory cards in SD, CompactFlash, Memory Stick or any related flash-based supplemental storage media;
    3. USB card readers that allow connectivity to a PC;
    4. Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function;
    5. PDAs, cell phones, and Smartphones with internal flash or hard drive-based memory that support a data storage function;

6. Digital cameras with internal or external memory support;
7. Removable memory-based media, such as rewritable DVDs, CDs, tapes, and floppy disks;
8. External hard drives;
9. Any hardware that provides connectivity to USB devices through means such as wireless or wired network access; and
10. Any applicable emerging technology.

B. Agency data must only be stored on agency-approved removable media.
C. Refer to Chapter 9 of the ESP for details regarding data encryption.
D. Guidelines for disposal/transfer of removable media must be followed. Refer to Chapter 15 of the ESP for details regarding hardware/media disposal.
E. Agencies utilizing removable media must consider:
    1. Implementing a management platform that allows centralized security policy administration to all agency-approved removable media.
    2. Implementing policy to define how removable media can be used within the agency.

Source: *Miss. Code Ann. § 25-53-1 to § 25-53-25*

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: General Security Policy

Rule 1.1 Authority. This document formally promulgates the State of Mississippi Enterprise Security Policy. For the purposes of this policy, security is defined as protection of the integrity, availability, and confidentiality of information; and the protection of Information Technology (IT) assets from unauthorized use, modification, damage, or destruction. It includes the security of primary and off-site IT facilities, data storage, and operations activities; computing, telecommunications, and applications-related services obtained from other government entities or commercial concerns; and Internet-related applications and connectivity.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.2 Scope. This policy applies to all Mississippi executive and judicial branch agencies and educational institutions (hereafter referred to collectively as "agencies"), as provided by law, that operate, manage, or use IT services or equipment to support critical state business and educational functions. Where conflicts exist between this policy and an agency's policy, the more restrictive policy will take precedence. This policy encompasses systems, automated and manual for which the agencies have administrative responsibility, including systems managed or hosted by third parties on behalf of the agencies. It addresses information, regardless of the form or format, which is created or used in support of business activities for the agencies. This policy applies to all users of agency information technology resources, including all agency employees, sub-contractors, temporary workers, and vendors.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.3 Purpose. The purpose of this policy is to define a set of 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 plans, policies, and procedures. The primary objectives of this policy are to:

C. Manage the risk of security exposure or compromise by focusing on the creation of a shared and trusted environment, with particular attention to:
    1. Common approaches to end-user authentication;
    2. Consistent and adequate network, server, and data management;
    3. Appropriate uses of secure network connections;
    4. Prevent unauthorized use or reproduction of copyrighted material by public entities; and
    5. Closing unauthorized pathways into the network and into the data pursuant to Mississippi Code Annotated § 25-53-5.

D. Establish an enterprise approach to security in state government that:
    1. Promotes an enterprise view among separate agencies;
    2. Requires adherence to a common security architecture and its related procedures;
    3. Recognizes an interdependent relationship among agencies, such that strengthening security for one strengthens all and, conversely, weakening one weakens all; and
    4. Assumes mutual distrust until proven friendly, including relationships with government, trading partners, and anonymous users to ensure secure interactions.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.4 Agency Directives. Each agency will establish a framework to initiate and control the implementation of security policies and standards within the agency. The head of each agency will ensure that an organization structure is in place for:

H. Operating in a manner consistent with the ITS Enterprise Security Policy;
I. Developing, implementing, maintaining, and complying with its own security plan and security policy;
J. Developing, implementing, maintaining, and testing security processes, procedures, and practices to protect and safeguard voice, video, and data computing and telecommunications facilities—including telephones, hardware, software, and personnel—against security breaches;
K. Training and educating all agency employees, associates, business partners, and others using its computers or networks to follow proper IT security procedures and standards;
L. Applying appropriate security measures when developing applications;
M. Implementing a security awareness program; and
N. Ensuring and overseeing compliance with this policy.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.5 ITS Security Officer; Role and Responsibilities. ITS has designated a Chief Information Security Officer (CISO) that is responsible for developing and maintaining the State of Mississippi Enterprise Security Policy. The ITS CISO and his staff will be responsible for:

I. Developing and maintaining the State of Mississippi Enterprise Security Policy.
J. Researching the IT industry for security related issues and determining how they affect the state IT infrastructure as a whole.
K. Participating in local and national security organizations for the purpose of sharing security information and developing best practice policy and procedure.
L. Working with state agencies on all security related issues.
M. Maintaining a state security listserve for the purpose of distributing security advisories and facilitating security discussion among the agency security contacts.
N. Maintaining a state security website for the purpose of sharing information, accessing contracts and documents, distributing security advisories, incident reporting, and education and awareness opportunities.
O. Working with agencies, technical support staff, and law enforcement where necessary, in the investigation of security incidents, intrusion attempts, and virus attacks. Reporting to agencies on these intrusion attempts and virus attacks.
P. Working with State Auditor's Office on IS audits as necessary.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.6 Agency Security Officer Roles and Responsibilities. ITS requires that each agency designate an individual as their agency's Security Officer. For agencies with small IT infrastructures, this designation could be a shared duty assumed by an existing member of the agency staff. For other agencies with very large/complex IT infrastructures, this designation requires that security be a major duty/responsibility for that individual. The agency Security Officer will be responsible for:

H. Developing and maintaining agency-specific security plans, policies, and procedures.
I. Interacting with ITS as the primary contact for security related issues.
J. Ensuring that their agency is adhering to the State of Mississippi Enterprise Security Policy.
K. Participating in the state information security listserve.
L. Researching IT industry for security related issues and how it affects their agency specifically.
M. Monitoring security issues within the agency's IT resources.
N. Facilitating the State Auditor's Information Systems Audit and the Third Party Risk Assessment.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.7 Auditing and Compliance; State Auditor's Role. Compliance with security policies is the responsibility of all state agencies. Any agency that fails to comply with security policies endangers everyone else in state government. Thus the following policy is established to clarify the role of the State Auditor and the Department of Information Technology Services, Information Security Division in auditing compliance:

G. The State Auditor will review how well agencies comply with security policies as part of their normal agency information systems auditing activities.
H. As a component of their standard Information Systems audit process, the State Auditor will consider the Enterprise Security Policy in the review of the systems, processes, and procedures that they will examine.
I. The State Auditor may request the assistance of the ITS Information Security Division in the performance of this normal audit function.
J. 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.
K. Upon determination of any non-compliance, the State Auditor may instruct the agency and/or the ITS Information Security Division to take necessary steps to become compliant.
L. Agencies should understand that failure to comply with the Enterprise Security Policy could result in a finding in the agency's audit report from the State Auditor.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.8 State, Federal, and Industry Guidelines. Based on its individual business needs and specific legal requirements, agencies may exceed the security requirements in this policy, but must, at minimum, achieve the security levels required by this policy. It is the responsibility of each agency to determine whether there are any guidelines or regulations outside the State of Mississippi Enterprise Security Policy they are required to meet. These guidelines may include:

G. Health Insurance Portability and Accountability Act (HIPAA) http://www.dhhs.gov/ocr/hipaa/
H. Federal Privacy Act http://www.justice.gov/opcl/privacyact1974.htm
I. Federal Educational Rights and Privacy Act (FERPA) http://www.ed.govpolicy/gen/guid/fpco/ferpa/index.html
J. PCI/DSS https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
K. Tax Information Security Guidelines for Federal, State and Local Agencies http://www.irs.gov/pub/irs-pdf/p1075.pdf
L. House Bill 583 of 2010: Breach of Security; Require notice http://billstatus.ls.state.ms.us/2010/pdf/history/HB/HB0583.xml

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.9 Security Policy Exemptions. This policy applies to Institutions of Higher Education except, pursuant to section § 25-53-25 of the Mississippi Code Annotated, when they develop security policies in lieu of the ITS Enterprise Security Policy that are:

C. Appropriate to their respective environments, and
D. Consistent with the intent of the ITS Enterprise Security Policy. Such higher education security policies must address:
    4. Appropriate levels of security and integrity for data exchange and business transactions;
    5. Effective authentication processes, security architectures(s), and trust fabric(s); and,
    6. Compliance, testing and audit provisions.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.10 Maintenance of Enterprise Security Policies, Standards, Guidelines and Recommendations. The revision date for this Enterprise Security Policy is ~~September 3, 2012~~ October 1, 2013. Technological advances and changes in the business requirements of state agencies will necessitate periodic revisions to enterprise security policies, standards, guidelines and recommendations. ITS is responsible for routine maintenance of these to keep them current.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 1.11 General Policy Requirements.

M. Each agency must operate in a manner consistent with the maintenance of a shared, trusted environment within state government for the protection of sensitive data and business transactions. Agencies may establish certain autonomous applications, including those hosted by an Applications Service Provider or other third party, outside of the shared, trusted environment, provided the establishment and operation of such applications follows all guidelines as set forth in this security policy and does not jeopardize the enterprise security environment, specifically:
    3. The security protocols (including means of secure transport, authentication, and authorization) relied upon by others; and
    4. The integrity, reliability and predictability of the state network infrastructure

N. Each agency must establish its secure state business applications within the criteria outlined in the ITS Enterprise Security Policy. This requires that all parties interact with agencies through a common security architecture and authentication process. ITS shall maintain and operate the shared state government network infrastructure necessary to support applications and data within a trusted environment.
O. Each agency that operates its applications and networks within the state government network infrastructure must subscribe to the following principles of shared security:
    5. Agencies shall follow security standards established for selecting appropriate assurance levels for specific application or data access and implement the protections and controls specified by the appropriate assurance levels;

6. Agencies shall recognize and support the state's standard means of authenticating external parties needing access to sensitive information and applications;
7. Agencies shall follow security standards established for securing servers and data associated with their applications; and
8. Agencies shall follow security standards established for creating secure sessions for application access.

P. Each agency must address the effect of using the Internet to conduct transactions for state business with other public entities, citizens, and businesses. Plans for Internet-based applications must be prepared and incorporated into the agency's security plan and submitted for review.

Q. Each agency must review its IT security processes, procedures, and practices at least annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment. Examples of these changes include modifications to physical facility, computer hardware or software, telecommunications hardware or software, telecommunications networks, application systems, organization, or budget. Practices will include appropriate mechanisms for receiving, documenting, and responding to security issues identified internally or by third parties.

R. Each agency must develop, implement, and maintain their individual agency IT security policy. Each agency will annually review, and revise (as needed) its security policy. 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.

S. Each agency must develop, implement, and maintain their individual agency IT security plan. Each agency will annually review, revise (as needed), and formally transmit its security plan to ITS.

4. Technological advances and changes in the business requirements will necessitate periodic revisions; therefore, agencies must review and update IT security plans at least annually and following any significant change to its business, computing, or telecommunications environment.
5. If an agency purchases IT services from another entity, the agency and the provider must work together to make certain the IT security plan for the provider fits within the agency's plan. If two or more agencies participate with each other in operating an information service facility, then the agencies must provide details within their individual agency security plans regarding these projects and ensure that their plans meets their mutual needs.
6. A portion of each agency's plan must promote security awareness by informing employees, associates, business partners, and others using its computers or networks about: security policies and practices, expectations of the users, and data handling procedures.

T. Agency heads are responsible for the oversight of their respective agency's IT security and will be required to confirm in writing that the agency is in compliance with this policy. The annual security verification letter must be submitted with the agency's security plan. The verification indicates review and acceptance of agency security processes, procedures, and practices as well as any updates to them since the last approval.

U. Each agency must obtain an IT security risk assessment from third-party security consultants at least once every three years. The agency will be required to submit a copy of the Executive Summary from the third party's assessment report to the ITS Information Security Division along with a copy of the agency's remediation plan for addressing issues identified within the assessment. Should critical or high-level risk be identified in the agency's report, the agency may be required to provide additional detailed information from the third party's full assessment report. Please be advised that any reports and/or documents resulting from a security risk assessment are classified as confidential and are not to be made available for public disclosure in accordance with Section 25-61-9 of the Mississippi code annotated. ITS recommends that agencies perform regular security assessments on their network throughout this three-year period, but it is not mandatory that they provide reporting for the additional security assessments.

V. Each agency may be subject to an Information Systems (IS) audit conducted by the State Auditor's Office. As part of the standard IS audit process, they will consider the Enterprise Security Policy as they review systems, processes, and procedures. The State Auditor may determine a special audit of an agency's IS 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 significant deficiencies revealed by the review or audit. To the extent that the audit documentation includes valuable formulate, designs, drawings, computer source codes, 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.

W. Each agency must ensure staff is appropriately trained in IT security policy, plans, and procedures. Each agency must make staff aware of the need for IT security and train them to perform the security procedures for which they are responsible. Agencies must participate in appropriate security alert response organizations at the state, regional, and national levels as required by their mission. At minimum, the agency must participate in the state's SecureNet listserve to receive security alert notifications.

X. The only permitted exceptions to the IT security policy of the State of Mississippi are those that are approved in writing by ITS for an agency's specific purpose and are only applicable to that agency's operations.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 2: State Network Resource Usage

Rule 2.1 Guest/public users must not be permitted access to the state network resources.

C. Any agency wishing to provide Internet access to a guest user must utilize one of the following approved methods:
    3. Installing separate equipment and a separate circuit for guest users. Contact ITS for more information on this method of connectivity.
    4. Tunneling guest user traffic to an ITS DMZ via the Cisco controller solution implemented by ITS. Contact ITS for more information on this method of connectivity.

D. Both methods require:
    3. No ports opened inbound to guest users.
    4. All guest user traffic must be filtered.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 2.2 Applications that pose a risk to the security of the State Network will not be permitted, including file transfer within Internet chat and peer to peer (P2P) file sharing programs.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 2.3 Each agency should consider developing an acceptable use policy (AUP) that defines the proper use of state resources by agency users. The AUP can protect users, partners, and agencies from illegal or damaging actions by individuals, either knowingly or unknowingly. Improper use of state resources exposes agencies to risks including virus attacks, compromise of state resources, and legal issues. ITS has developed an AUP for its users and it can be viewed at: http://www.its.ms.gov/Policies/Documents/itsusepolicy.pdf

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 2.4 Each agency must develop a policy that defines the use of personal devices (i.e. mobile devices, minis, laptops, personal computers) on state systems. At minimum, this policy must require those devices to be subject to the same security requirements as state owned devices. It is recommended that the agency personal device policy include information describing how personal devices may be monitored and agency expectations regarding user cooperation in the investigation of a security breach, related to state information, where the personal device is a potential source for the breach. Additionally, it is recommended that the agency require the user to sign a letter or agreement acknowledging that they agree and understand the agency personal device policy

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 3: Incident Reporting

Rule 3.1 Each agency must report all information security incidents to the ITS Information Security Division (ISD) as soon as possible.

Information security incidents result from a validation of an information security event. Information security events are defined as any violation of computer security policies, network integrity, data confidentiality, or standard computer security practices.

Detailed reporting procedures and a description of reportable events are provided in the ISD Cyber Security Incident Reporting Guidelines document. State employees can access this document from the ITS website.

E. Each agency must establish security event/incident response procedures that define the actions to be taken when a security event/incident occurs.
F. Each agency is responsible for assessing the significance of a security incident within their organization and for providing this information to ISD based on the business impact on affected resources and the current and potential technical effect of the incident (e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of sensitive information, or propagation to other networks).
G. Each agency must implement a policy requiring all agency users to report suspected security events/incidents to an appropriate level supervisor, manager, or security officer within their agency. Each agency must train their users on the procedures for reporting a suspected security event, security policy violation, state or federal law violation, theft, damage, or action placing state resources at risk.
H. Each agency is responsible for contacting the appropriate law enforcement and investigative authorities if criminal action is suspected.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 4: Data Classification

Rule 4.1 Data must be properly managed from its creation, through authorized use, to proper disposal. This data classification policy provides a high-level guideline to state agencies for the purpose of understanding and managing data and information assets with regard to the level of protection required. This policy requires that all data be classified on an ongoing basis and managed based on its confidentiality, integrity, and availability characteristics.

J. Each agency must establish a data classification policy and shall serve as a classification authority for the data and information that it collects or maintains in satisfaction of its mission.
    4. Data classifications are a prerequisite to establishing agency guidelines and system requirements for the secure generation, collection, access, storage, maintenance, transmission, archiving, and disposal of state data.

    5. The data classification identifies how sensitive the data is with regard to unauthorized disclosure. Data should be assigned one of three classifications:

a. ***Public:*** The "public" classification includes information that must be released under Mississippi open records law or instances where an agency unconditionally waives an exception to the open records law.
b. ***Limited Access:*** The "limited-access" classification applies to information that an agency may release if it chooses to waive an exception to the open records law and places conditions or limitations on such a release.
c. ***Sensitive:*** The "sensitive" classification applies to information, the release of which is prohibited by state or federal law. This classification also applies to records that an agency has discretion to release under open records law exceptions but has chosen to treat as highly confidential.

6. In addition to the data classification, all data must also have a designated data owner. The data owner will be responsible for assigning data classification regarding their data.

K. State and federal law may require that certain types of data be classified in a particular manner. Each agency shall determine if there are state or federal legal requirements for classifying the data and shall assign the classification(s) as required by law. (i.e. HIPAA, PCI, etc.)
L. Each agency must establish a process to regularly review the appropriateness of the assigned data classifications and adjust classifications in the event of regulatory changes affecting an agency's management of information under its control.
M. Each agency must ensure that data compiled from multiple sources is classified with at least the most secure classification level of any individually classified data in the set.
N. Each agency must ensure that data shared with other agencies is consistently classified and protected in accordance with a documented agreement detailing, at a minimum, data treatment requirements.
O. Each agency must ensure that sensitive data is secured in accordance with applicable agency requirements, federal or state regulations/guidelines, and the enterprise security policy.
P. All reproductions of data in its entirety must carry the same data classification as the original. Partial reproductions of data need to be evaluated to determine if new classifications are warranted.
Q. If an agency is unable to determine the data classification of data, the data should be assumed to have high classification requirements and, therefore, is subject to a data classification of "sensitive".
R. All personally identifiable information (PII) must be classified as "sensitive".

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 5: Servers

Rule 5.1 Each agency is required to "harden" their servers. Hardening these servers includes:

J. Regularly installing all service packs, patches, and updates after appropriate integration testing.
K. Disabling all unnecessary services, devices, and accounts.
L. Enabling appropriate logging and routine log activity review procedures.
M. Establishing adequate access and control mechanisms.
N. Ensuring user authentication and data protection.
O. Performing routine scans for vulnerabilities and configuration weaknesses.
P. Setting security parameters and file protections.
Q. Enabling firewall software on the server.
R. Maintaining virus scanning software on all servers.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 5.2 Proper physical location of the server must be considered. Refer to chapter 12 of the ESP for more information about physical access.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 5.3 Internet-facing servers that reside on the State Network must be properly secured to preserve the integrity of the network. Inbound connections from the Internet or any third party network will be made using HTTP or HTTPS through enterprise reverse proxy devices in the ITS DMZ.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 6: Email

Rule 6.1 To increase security and limit spam and emailed viruses, ITS has implemented and maintains mail relays on the inside and outside of the firewall. All mail bound for state domain email addresses must come through the outside mail relay and be "relayed" to the inside mail relays. The inside mail relay forwards the mail on to the appropriate mail server. All outbound mail going out passes through the inside mail relay before being forwarded to the Internet. For this reason, agencies must adhere to the following guidelines for mail:

E. No direct SMTP to and/or from the Internet. Agencies must utilize the ITS maintained mail relays for mail traveling in both directions.
F. No POP or IMAP from Internet to mail servers inside state network. Agencies must utilize a secure web interface (HTTPS) to access mail.
G. No POP or IMAP from state network to private mail accounts on Internet. Agencies must utilize a web interface (HTTP/HTTPS) to access this mail.
H. ITS recommends that Agencies forward all mail through to the inside mail relay and restrict TCP 25 inbound and outbound in their firewalls to the relays' addresses.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 6.2 Each agency must establish policies to help employees use email properly, to reduce the risk of intentional or inadvertent misuse, and to ensure that official records transferred via electronic mail are properly handled. Principle priorities include the following:

E. Email communications must not be unethical, fraudulent, harassing, obscene, or be perceived as a conflict of interest.
F. User must be instructed of the risk of opening file attachments they were not expecting to receive.
G. Email must be used to conduct official business only.
H. Clear text emails must not contain sensitive information. If sensitive information must be communicated using email, the email must be encrypted both in transport and at rest.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 7: Virus Prevention

Rule 7.1 Agencies are required to have a virus prevention program that includes:

J. Maintaining virus scanning software on all servers and workstations.
K. Keeping virus signature files and scanning engines updated on a schedule relevant to the system. Workstations must be updated at least weekly, and servers must be updated at least daily. A more stringent schedule may be adopted if the agency deems the machine a higher risk.
L. Scanning all file attachments sent or received via e-mail using current anti-virus software.
M. Scanning all removable media upon connection/ insertion using current anti-virus software.
N. Immediately removing any infected workstation or server from the network until the virus has been cleaned.
O. Maintaining copies of virus-detection tools offline.
P. Keeping all servers and workstations current with operating system and software security patches.
Q. Disabling AutoPlay on all workstations and laptops.
R. Reporting all virus activity that is not automatically cleaned by the virus protection software to ISD as a security incident. Refer to Chapter 3 of the ESP for details regarding incident reporting.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 7.2 ITS will monitor for network activity that indicates the presence of malicious code and upon detection will perform the following actions:

C. For isolated infections, ITS will block access to the state network for infected workstations or servers and notify the agency contact. Once the agency contact confirms that the workstation or server has been cleaned, ITS will remove the

block. Detailed information regarding this process is provided in the ISD-Ticket Response Guidelines document. State employees can access this document from the ITS website.

D. For cases of infection within an agency that have the potential to impact other agencies, ITS will limit or remove connections to the state network for the infected agency. Such drastic action will be considered any time the availability, reliability, or integrity of the state network is at risk, but ITS will attempt to work with the infected agency to find a mitigating alternative prior to removing access.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 8: Firewalls

Rule 8.1 ITS will maintain a perimeter firewall between the State Network and the Internet. This firewall will provide address-translation to public space for state agencies.

E. Inbound connections from the Internet will be restricted to only ports TCP 80 and TCP 443, for only HTTP and HTTPS protocols. No other inbound-initiated ports will be allowed to servers residing on the State Network unless entering the state network over a VPN.
F. ITS will maintain a DMZ for applications that meet the following criteria:
    4. Require inbound connections that are not HTTP or HTTPS
    5. Declared business-critical by both the agency and ITS
    6. Deemed as unsuitable for a VPN by ITS

G. All applications utilizing the ITS DMZ must reside in the State Data Center.
H. Outbound connections from the State Network will be largely unrestricted. Exceptions to this include LAN protocols, ICMP, and ports known for propagating malicious code.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 8.2 Each agency is required to implement a firewall at the perimeter of their network, to secure the LAN from any traffic originating within the State Network. Each agency should define a rule set for their firewall that is as restrictive as possible, permitting the minimum services required for proper operation of inter-agency communication. All services not required for proper operation should be denied by the rule set.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 8.3 Firewalls must only be managed using secure protocols such as SSH or HTTPS, and management should be allowed only from selected agency workstations.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 8.4 Firewall event logging must be enabled and the logs maintained for at least 30 days.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 9: Data Encryption

Rule 9.1 ITS requires that all sensitive data be encrypted using industry standard algorithms Triple DES, AES, or SSL/TLS when traveling to/from un-trusted networks and/or entities.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 9.2 If an agency Internet-facing server gathers or transmits sensitive data, the application must use, at minimum, SSL for the transaction. The agency must acquire the Certificate Authority signed certificate for this server from ITS.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 9.3 Each agency should consider encrypting the transmission of all sensitive data.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 9.4 Each agency must encrypt sensitive data stored on any of their local systems. Agencies must also ensure that any sensitive data on systems located offsite is properly encrypted.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 10: Remote Access

Rule 10.1 The following policies address connectivity into the state network from any entity that resides outside the state network. This includes third party entities' connectivity into the state network via both the public Internet and private circuits.

J. 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.

K. 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).
    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.

L. 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. It should be understood that 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 while the tunnel is connected (as defined above) does not meet the requirements or intent of this security policy.

M. 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.

N. ITS maintains Cisco VPN termination devices to establish client-based and LAN-to-LAN VPNs for access to resources on the state network.

1. All LAN-to-LAN VPNs will be implemented using the IPSec protocol.
2. Any third party entity that needs an inbound connection to the state network must provide and maintain a compatible industry-standard IPSec-capable VPN hardware/software solution at their end of the connection. VPNs must be addressed using public IP addresses registered to that entity, including the peer address and any networks at the third party that will be encrypted by the tunnel. The ITS side of the connection will adhere to the same requirements, but with the public IP addresses provided by ITS.
3. Client-based VPNs may be implemented with IPSec or SSL.

O. At no time may an agency permit a third party entity to connect directly to their local area network behind the state's border firewall and/or the agency's firewall. This includes terminating third party circuits behind ITS and agency firewalls and/or utilizing a PC remote control product (unless approved in writing by ITS) via a dialup or Internet connection. This does not include remote support applications that require real-time interaction by the agency end user, such as GoToAssist and WebEx.

P. If an agency provides dial-in access to agency personnel either via a remote access service or PC modem on their LAN or via an outsourced remote access service, the agency must implement a firewall to control access to and from the local area network by the dial users. The agency will be held responsible for any dial user that uses their facilities to access and manipulate or abuse any other facility.

Q. It is essential that all access to the state's network be terminated immediately upon the retirement, resignation, dismissal, end of contract, or any and all other actions that signal that the requirements for having a connection are no longer being met.

R. At no time should any employee, vendor or account holder provide their login, user information or password to anyone. Employees, vendors or account holders are assigned individual accounts that must never be treated as a shared account.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 11: Passwords

Rule 11.1 ITS requires, at minimum, that each state agency utilize the following guidelines when developing their password policy. Each agency must enforce their developed password policy and educate their users on the choice and protection of passwords.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 11.2 Each agency must adopt the following guidelines for password administration:

G. Automated password input must not be allowed, except for simplified/single sign on systems that have been approved by ITS
H. Passwords must not be stored in clear text on hard drives or any other electronic media. If stored on electronic media, passwords must be classified as sensitive. Refer to Chapter 9 of the ESP for details regarding data encryption.
I. Access to password-protected systems must be timed out after an inactivity period of thirty (30) minutes or less.
J. Passwords for administrative accounts and accounts with access to sensitive data must be treated with a higher level of security, including:
    1. Requiring password changes every thirty (30) days
    2. Consideration of two-factor authentication

K. Third-party support accounts must be disabled or deleted when not in use.
L. Immediately revoke access when an account owner leaves or is terminated.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 11.3 Each agency must enforce the following guidelines for user password creation:

I. Passwords must contain at least 8 characters.
J. Passwords must contain a combination of lower case letters, upper case letters, numbers, and at least one symbol.
K. Passwords must not contain the user ID.
L. Passwords must not include personal information about the user that can be easily guessed: user's name, spouse's name, kid's name, employee number, social security number, birth date, telephone number, city, etc.
M. Passwords must not include words from an English dictionary or foreign-language dictionary.
N. Passwords must not contain proper names, including the name of any fictional character or place.
O. Passwords must not contain any simple pattern of letters or numbers such a "qwertyxx", "12345678", or "xyz123xx."
P. Passwords must not be trivial, predictable or obvious.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 11.4 Each agency must instruct their users to follow these guidelines for the purpose of protecting passwords:

I. Passwords must not be disclosed to anyone except in emergency circumstances or when there is an overriding operational necessity.
J. Hard copies of passwords (i.e. printed out or written down) should be considered sensitive.
K. Passwords must not be sent in clear text over the network. Secure Shell (SSH) and HTTPS must replace Telnet and HTTP for authentication.
L. Passwords must be unique per user.
M. The password change interval is a maximum of ninety (90) days; however, ITS recommends that agencies consider using a 30 or 60 day interval depending on the classification of their data. Password reuse should be minimized or prohibited.
N. Default passwords must be changed.
O. Passwords must be required on all user accounts.
P. Passwords suspected to be stolen or cracked must be changed immediately and notification must be given to the user's supervisor and system administrator.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 11.5 For users that have access to sensitive data or that have system administrator rights, agencies must consider using two-factor authentication. Two-factor authentication is a system wherein two different factors are used in conjunction to authenticate.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 12: Physical Access

Rule 12.1 All data center facilities must be physically protected in proportion to the criticality of the business functions and associated systems, assets, and infrastructure.

E. Any computing resource connected to an agency LAN or to the State Network must be placed in an area that can be locked. Any PC that is left unattended during the day must be logged out or locked when inactive. Refer to Chapter 11 of the ESP for details regarding password requirements.
F. At minimum, wiring closets must be kept in an area that can be locked.
G. At minimum, State Network routers or switches must be kept in an area that can be locked. This includes remote offices.
H. Agencies should ensure that all laptops are stored in secure locations.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 12.2 Agencies with larger computer installations must:

H. Protect access with an access control system, normally a card access system.
I. Establish procedures for granting, modifying, and revoking access.
J. Establish procedures for recording information (date, time, etc.) to track access.
K. Require security related clearance as a result of employment. (For example, all ITS employees that have access to State Data Center facilities are sworn in as Information Confidentiality Officers as defined by legislation and are subject to background checks).

L. Use cameras to record activity in and around computer installation.
M. Establish a policy for archiving access system and video data. Agencies must archive access system and video data for a minimum period of 30 days.
N. Restrict visitors in the computer facilities. Visitors that are allowed access must sign a sign-in/out log and must be accompanied by an authorized staff member.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 12.3. Agencies with smaller computer installations must:

D. Protect access with locked rooms, at minimum.
E. Establish procedures for granting, modifying, and revoking access.
F. Establish procedures for recording information (date, time, etc.) to track access.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 12.4 Agencies should adhere to the following miscellaneous physical security guidelines:

D. Each agency should locate alternate space that meets the same physical security requirements for a business recovery site. This site should be accessible 24/7/365.
E. Backup and recovery materials (tapes, manuals, etc.) must be kept at a site that meets all security measures defined in this document. This site should be accessible 24/7/365.
F. Areas housing environmental or electrical systems critical to computer facilities should be in a location that meets all security measures defined in this document.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 13: Wireless Access

Rule 13.1 The following policies address security and data integrity measures required for implementing and securing wireless local area networks that reside within the state network.

D. Any unauthorized and/or neglectful installations of wireless networks that expose the state's network infrastructure to intruders and/or attacks may result in that agency's connection to the state network being isolated.
E. Maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems.
F. Agencies must assess risks more frequently and test and evaluate system security controls more frequently when wireless technologies are deployed.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Rule 13.2 At minimum, the following security standards and network configurations are required for the deployment and operation of all wireless network installations:

K. The placement of wireless LAN Access Points (WAP) must be strategically located to minimize the interception of wireless signals by unauthorized individuals. The range of the signal must also be tested to ensure that signals are not being transmitted outside the intended coverage area.

L. All WAP installations must use encryption. WPA Version 2 with AES is the minimal level of acceptable encryption. WEP and WPA (version 1) are not permitted.
M. WPA Version 2 may be deployed in either "PSK mode" or "Enterprise mode" with specific requirements for each mode.
    1. PSK mode deployment requirements:
        a. The "key" or "pass-phrase" should be known and kept securely by as few personnel as possible.
        b. The "key" or "pass-phrase" should be changed regularly. Regularly is defined as every three months for minimum standards, however, it is recommended to be changed every month.
        c. Very strong password creation practices should be followed when creating WPA-PSK passwords. At minimum, 16 characters with a combination of lower case letters, upper case letters, numbers, and symbols should be used.

    2. Enterprise mode deployment requirements
    Enterprise mode indicates that, in addition to encryption keys on the WLAN, user credentials are required for access. This mode is recommended as more secure than PSK mode, due to the second factor being required. Two known methods for implementing enterprise mode are:
        a. Radius server with rolling PSK.
        b. Manual change of PSK as described in PSK mode, with network access control deployed.

N. All WAP configuration parameters (Service Set Identifier (SSID), keys, passwords, channels, etc) that can be changed from the default manufacturer settings must be changed from the default.
O. WAPs must be connected to a switch and not a hub.
P. Physical security of WAPs must be maintained to protect the WAP from theft or access to the data port.
Q. Open broadcasting of the SSID must be disabled.
R. Wireless encryption protocols only secure the LAN radio transmissions. Any sensitive data must still be handled with the appropriate network-transmission protocols. Refer to Chapter 9 of the ESP for details regarding data encryption. Each agency should consider the use of VPNs for specific users or network segments that need to transmit sensitive data.
S. Software and firmware updates from the wireless manufacturer should be applied to the WAP and affected wireless cards as soon as possible after release.
T. Additionally, the following wireless security best practices are recommended for deployment and operation of a wireless network.
    1. All WAP installations should be inventoried and the area in which the wireless LAN is installed should be regularly inspected for unauthorized WAPs or other devices not part of the approved installation. The network should be regularly inspected both physically and electronically using sniffing tools to uncover rogue WAPs and devices.

2. The network should be scanned on a regular basis to detect unauthorized clients.
3. Agencies with large, complex scale wireless implementations should consider using a solution that provides for centralized configuration and management of the wireless access point rather than individually maintaining each WAP.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 14: Laptop and Mobile Device Usage

Rule 14.1 Each agency must adhere to the following policies for mobile devices with sensitive data. A mobile device is defined as any electric and/or battery operated device that can be easily transported and that has the capability for storing, processing, and/or transmitting data including Laptops, Portable Digital Assistants (PDAs), Tablet/Mini PCs, Blackberries, SmartPhones, and Hand-Held PCs. It is recommended that agencies consider enforcing some or all of these policies for any mobile device regardless of classification of the data.

H. Agencies employing the use of mobile devices for access to agency systems or storage of agency data must appropriately secure those devices to prevent sensitive data from being lost or compromised, to reduce the risk of spreading viruses/malware, and to mitigate other forms of abuse.
I. While traveling and using a mobile device in public places, never leave the device unattended and take precautions to avoid the risk of unauthorized persons viewing information on-screen.
J. Agencies must consider software that aids in tracking and recovery of the mobile device if lost or stolen.
K. Agencies that allow the use of mobile devices for access to state data, must consider implementing a management platform that allows them to administer the appropriate security policy to all devices supported by the agency.
L. Access Control
    1. Prohibit users from downloading, running, and/or installing software and applications or enabling unauthorized protocols or services without agency IT approval and assistance.
    2. Mobile device users must minimize the potential loss of data via WiFi, 3G, or Bluetooth connections to their device by configuring them in a secure manner or turning those services off when not in use.
    3. Disable boot-up capabilities of other drives. Disabling the secondary boot drive sequence hinders the ability to access the system from a secondary drive.
    4. Rename the Administrator Account using a non-descript name.
    5. Prevent the last user name from displaying in the login dialog box.
    6. When connected to the state network, ensure only one active connected network interface is enabled at a time. For example, if WiFi is enabled, then other access methods are disabled.

7. Establish hard drive and/or BIOS password standards for the agency or each department of the agency. Enable these features on each mobile device and configure a password per this standard.

M. Authentication

4. All mobile devices must require authentication before accessing state resources/services. Where mobile devices will have access to sensitive information, the agency should consider two-factor authentication and at minimum use strong authentication/password characteristics.
5. Mobile devices should be configured to timeout after 30 minutes of inactivity and require re-authentication. Authentications must not be disabled on the mobile device.
6. Agencies should require users to log out or turn mobile devices off if leaving the device unattended.

N. Encryption

5. Refer to chapter 9 of this document for information regarding data encryption.
6. Many mobile devices support the use of removable storage devices to store data. If sensitive data is stored on removable storage devices, the data must be encrypted.
7. Consider implementing whole disk encryption. Whole disk encryption is preferred as it "locks" the hard drive preventing it from being accessed by physically installing it in similar equipment.
8. Consider installing disk wiping technology that remotely wipes the mobile device clean in the event of loss or theft.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25.*

Part 1 Chapter 15: Disposal of Hardware/Media

Rule 15.1 Each agency must determine if hardware/media contains any sensitive data prior to disposal (scrap, destroy, transfer or rental/lease return). If hardware/media contains sensitive data, one of the following methods must be used prior to disposal.

C. Physical Destruction

This is the primary method that should be used for the disposal of data storage devices containing sensitive data. The intent is to completely destroy the data storage device beyond any possibility of data recovery.

1. The agency should perform a complete and permanent elimination of data on the data storage device.
2. Physical destruction of data storage devices is performed by shredding, disintegrating, incinerating, pulverizing, and melting the data storage device
3. If a third party is contracted for the disposal of the data storage device, a certificate of destruction must be obtained.

D. Overwriting
This method should be used in cases of exception when physical destruction of data storage devices is not reasonable or is prohibitive.
    1. Agencies may sanitize magnetic media (i.e. hard disk) by an overwriting process, whereby a software utility writes a combination of characters (usually 0s and 1s) over each location on the data storage device multiple times.
    2. This process obscures the previous information, rendering the data unreadable. Agencies must overwrite the device a minimum of three times prior to disposal.
    3. To verify the overwriting process, agencies should attempt to recover the data by one or more commercially available "data recovery utilities".
    4. Simply erasing and reformatting a data storage device is not a permissible method of sanitizing a data storage device before disposal.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25*

Rule 15.2 Each agency must erase all data and configuration information, regardless of the classification of data, prior to disposal (scrap, destroy, transfer, or rental/lease return) of hardware.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25*

Part 1 Chapter 16: Application Assessment and Certification

Rule 16.1 Each agency must perform security assessments on all new applications to ensure key application 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.

C. Agencies should use one or more of the following application security assessment methods:
    1. Contract with a third-party for assessment services
    2. Perform Internal application security assessments
    3. Utilize application security assessment software

D. At minimum, the following vulnerabilities must be assessed.
    1. Un-validated input
    2. Broken access control
    3. Broken authentication and session management
    4. Injection flaws
    5. Improper error handling
    6. Insecure configuration management
    7. Insecure storage
    8. Cross-Site scripting (XSS)

9. Insecure direct object references
10. Cross-Site request forgery (CSRF)
11. Insufficient transport layer protection
12. Unvalidated redirects and forwards

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25*

Rule 16.2 Each agency must document their application security assessment process/results prior to deploying new applications. Agencies must include all application assessment documentation to ITS as part of the submission package satisfying the mandatory third-party security risk assessment. Refer to Chapter 1 of the ESP for details regarding security risk assessments.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25*

Rule 16.3 Application security assessments must performed when an application is modified or updated. ITS recommends that agencies perform application assessments on a regular basis.

B. Follow-up application security assessment documentation must be submitted to ITS as part of the submission package satisfying the mandatory third-party security risk assessment. Refer to Chapter 1 of the ESP for details regarding security risk assessments.

Source: *Miss. Code Ann.* § *25-53-1 to § 25-53-25*

Part 1 Chapter 17: Removable Media

Rule 17.1 Agencies must adhere to the following policies for removable media regardless of classification of the data being stored.

F. Removable Media is defined as a device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This removable media policy pertains to, but is not limited to all devices and accompanying media that fit the following criteria:
    1. Portable USB-based flash drives, also known as thumb drives, jump drives, or key drives;
    2. Memory cards in SD, CompactFlash, Memory Stick or any related flash-based supplemental storage media;
    3. USB card readers that allow connectivity to a PC;
    4. Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function;
    5. PDAs, cell phones, and Smartphones with internal flash or hard drive-based memory that support a data storage function;
    6. Digital cameras with internal or external memory support;
    7. Removable memory-based media, such as rewritable DVDs, CDs, tapes, and floppy disks;

8. External hard drives;
9. Any hardware that provides connectivity to USB devices through means such as wireless or wired network access; and
10. Any applicable emerging technology.

G. Agency data must only be stored on agency-approved removable media.
H. Refer to Chapter 9 of the ESP for details regarding data encryption.
I. Guidelines for disposal/transfer of removable media must be followed. Refer to Chapter 15 of the ESP for details regarding hardware/media disposal.
J. Agencies utilizing removable media must consider:
    1. Implementing a management platform that allows centralized security policy administration to all agency-approved removable media.
    2. Implementing policy to define how removable media can be used within the agency.

Source: *Miss. Code Ann. § 25-53-1 to § 25-53-25*