## 1. Authority

This document formally promulgates the Mississippi Department of Information Technology Services (ITS) 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.

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 functions. The provisions of § 25-53-1 to § 25-53-25 of the Mississippi Code Annotated details the powers and duties of ITS, including the authority to develop statewide or interagency information services and technical policies, standards and procedures. All agencies will adhere to the requirements and guidelines of this policy, using them as minimum standards with which to develop, implement, and maintain their individual agency IT security plans. Each agency is responsible and accountable for compliance with its own security plan and is required to educate all employees, both government and contract, to follow proper IT security procedures. Each agency will annually review, revise (as needed), and formally transmit its security plan to ITS. Revisions to agency security plans must incorporate relevant technological advances in the broad areas of IT, changes in agency business requirements, and changes in the agency's IT environment. As a component of their standard Information Systems audit process, the State Auditor's Office will consider the Enterprise Security Policy in the review of the systems, processes, and procedures that they will examine. 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.

## 2. Purpose

2.1. The state's transition from a proprietary network utilizing dedicated leased facilities to IP-based networks, including the Internet, for conducting vital public business has highlighted the following security concerns:

2.1.1. Information Integrity - Unauthorized deletion, modification or disclosure of information;

2.1.2. Misuse - The use of information assets for other than authorized purposes by either internal or external users;

2.1.3. Information Browsing - Unauthorized viewing of sensitive information by intruders or legitimate users;

2.1.4. Penetration - Attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs;

2.1.5. Computer Viruses – Attacks using viral code that reproduces itself by modifying other programs, spreading across multiple programs, data files or devices on a system or through multiple systems in a network, that may result in the destruction of data or the erosion of system performance;

2.1.6. Fraud - Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in financial loss or embarrassment to the organization;

2.1.7. Component Failure - Failure due to design flaws or hardware/software faults that lead to denial of service or security compromises through the malfunction of a system component; and

2.1.8. Unauthorized additions and/or changes to infrastructure components.

2.2. Because information technology security planning is primarily a risk management issue, this policy and its associated standards and guidelines focus on the creation of a shared and trusted environment, with particular attention to:

2.2.1. Common approaches to end-user authentication;

2.2.2. Consistent and adequate network, server, and data management;

2.2.3. Appropriate uses of secure network connections; and

2.2.4. Closing unauthorized pathways into the network and into the data pursuant to Mississippi Code Annotated, § 25-53-3.

2.3. Such an environment is made possible through an enterprise approach to security in state government that:

2.3.1. Promotes an enterprise view among separate agencies;

2.3.2. Requires adherence to a common security architecture and its related procedures;

2.3.3. Recognizes an interdependent relationship among agencies, such that strengthening security for one strengthens all and, conversely, weakening one weakens all; and

2.3.4. Assumes mutual distrust until proven friendly, including relationships within government, with trading partners, and with anonymous users.

2.4. In response to these threats and to assist state agencies in mitigating associated risks, ITS requires that agencies take steps necessary to initiate an enterprise-wide approach to:

2.4.1. Ensure secure interactions between and among governmental agencies take place within a shared and trusted environment;

2.4.2. Ensure secure interactions between and among business partners, external parties and state agencies utilize a common authentication process, security architecture, and point of entry;

2.4.3. Prevent misuse of, damage to, or loss of IT hardware and software facilities;

2.4.4. Ensure employee accountability for protection of IT assets; and

2.4.5. Prevent unauthorized use or reproduction of copyrighted material by public entities.

2.5. Accordingly, ITS directs state agencies to:

2.5.1. Operate in a manner consistent with the ITS Enterprise Security Policy;

2.5.2. Develop, implement, maintain, and test 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;

2.5.3. Train staff to follow security procedures and standards;

2.5.4. Apply appropriate security measures when developing transactional Internet-based applications, including but not limited to electronic commerce (e-commerce); and

2.5.5. Ensure and oversee compliance with this policy.

## 3. Scope

These standards apply to all executive and judicial branch agencies and educational institutions, as provided by law, that operate, manage, or use IT services or equipment to support critical state business and educational functions.

## 4. Policy

4.1. It is the IT security policy of the State of Mississippi that:

4.1.1. Each agency shall 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:

4.1.1.1. The security protocols (including means of secure transport, authentication, and authorization) relied upon by others; and

4.1.1.2. The integrity, reliability and predictability of the State network infrastructure.

4.1.2. Each agency shall 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.

4.1.3. Furthermore, each agency that operates its applications and networks within the MS state government network infrastructure must subscribe to the following principles of shared security:

4.1.3.1. 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;

4.1.3.2. Agencies shall recognize and support the state's standard means of authenticating external parties needing access to sensitive information and applications;

4.1.3.3. Agencies shall follow security standards established for securing servers and data associated with the secure application; and

4.1.3.4. Agencies shall follow security standards established for creating secure sessions for application access.

4.1.4. 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 transactional applications, including but not limited to e-commerce, must be prepared and incorporated into the agency's security plan and submitted for review.

4.1.5. Each agency must ensure staff is appropriately trained in IT security 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 and regional levels.

4.1.6. 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 by third parties.

4.1.7. 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.

4.1.8. 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 to ITS by January 31st each year. The verification indicates review and acceptance of agency security processes, procedures, and practices as well as any updates to them since the last approval.

4.1.9. Agencies 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.

4.2. 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.

## 5. 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:

5.1. Appropriate to their respective environments, and

5.2. Consistent with the intent of the ITS Enterprise Security Policy. Such higher education security policies must address:

5.2.1. Appropriate levels of security and integrity for data exchange and business transactions;

5.2.2. Effective authentication processes, security architecture(s), and trust fabric (s); and,

5.2.3. Compliance, testing and audit provisions.

## 6. Maintenance of Policies, Standards, Guidelines and Recommendations

Technological advances and changes in the business requirements of State agencies will necessitate periodic revisions to policies, standards, guidelines and recommendations. ITS is responsible for routine maintenance of these to keep them current. Major policy changes will require the approval of ITS.

## 7. Security Plan; Review, Schedule and Updates

7.1. 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.

7.2. 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 develop a joint IT security plan which meets their mutual needs.

7.3. A part of the agencies' plans must promote security awareness by informing employees, associates, business partners, or others using its computers or networks about security policies and practices, what is expected of them, and how they are to handle the information.

## 8. Agency Data Classification

8.1. Purpose

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 their level of confidentiality and sensitivity. Increased connectivity of computers and databases makes more data available to individuals, businesses and agencies. As a result, the potential for unauthorized disclosure, modification or destruction of personal, financial, medical, business and other types of data also has increased. There may or may not be laws that regulate the use of particular data, and agencies may not be certain how to respond to apparent conflicts between privacy, open records laws and the need to maintain safety and security. Data classification is a process that identifies what information needs to be protected against unauthorized access, use, or abuse.

8.2. Policy

State agencies shall 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.

8.2.1. The classification of data is a critical tool in defining and implementing the correct level of protection for state information assets. Such 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.

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

8.2.2.1. ***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.

8.2.2.2. ***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.

8.2.2.3. ***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 the information as highly confidential.

8.2.3. State and federal law may require that certain types of data be classified in a particular manner. Agencies 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)

8.2.4. Agencies must establish a process to regularly review the appropriateness of the assigned data classifications and to adjust classifications in the event of regulatory changes affecting an agency's management of information under its control.

8.2.5. The agency shall ensure that data compiled from multiple sources is classified with at least the most secure classification level of any individually classified data.

8.2.6. The agency shall 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.

8.2.7. The agency shall ensure that sensitive data is secured in accordance with applicable agency requirements, and federal or state regulations and guidelines, and the enterprise security policy.

8.2.8. The agency shall ensure that data access requirements are incorporated into contractor/vendor service level agreements and contract terms and conditions as they relate to classified data.

## 9. Security Officers; Role and Responsibilities

9.1. 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:

9.1.1. Developing and maintaining the State of Mississippi Enterprise Security Policy

9.1.2. Researching the IT industry for security related issues and determine how it effects the State IT infrastructure as a whole

9.1.3. Participating in local and national security organizations for the purpose of sharing security information and developing best practice policy and procedure

9.1.4. Working with state agencies on all security related issues

9.1.5. Maintaining a State Security Listserve for the purpose of distributing security advisories and facilitating security discussion among the agency security contacts.

9.1.6. 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.

9.1.7. 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.

9.1.8. Working with State Auditor's Office on IS audits as necessary.

9.2. 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:

9.2.1. Developing and maintaining Agency-specific security policies and procedures

9.2.2. Be ITS's primary contact for security related issues

9.2.3. Ensure that their agency is adhering to the State of Mississippi Enterprise Security Policy

9.2.4. Participate in the State Information Security Listserve

9.2.5. Research IT industry for security related issues and how it effects their agency specifically

9.2.6. Monitor security issues within the agency's IT resources

9.2.7. Facilitate the State Auditor's Information Systems audit and the Third Party Risk Assessment

**10. 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:

10.1. The State Auditor will review how well agencies comply with security policies as part of their normal agency Information Systems auditing activities.

10.2. The State Auditor may request the assistance of the ITS Information Security Division in the performance of this normal audit function.

10.3. The State Auditor may request and review copies of an agency's IT Security Risk Assessment separate or in conjunction with normal agency audit processes.

10.4. 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.

11. **Federal Guidelines**

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:

11.1. Health Insurance Portability and Accountability Act (HIPAA) http://www.dhhs.gov/ocr/hipaa/

11.2. Federal Privacy Act http://www.usdoj.gov/oip/04_7_1.html

11.3. Federal Educational Rights and Privacy Act (FERPA) http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

11.4. Department of Defense 5220.22 http://www.dtic.mil/whs/directives/corres/html/522022m.htm

11.5. PCI/DSS https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

12. **Technical Documents**

**The technical documents can be found on the ITS website at: www.its.ms.gov/services_security**

12.1. Technical Document Directory: PSG 100-09.1

12.2. Web Servers: PSG 100-09.2

12.3. Email: PSG 100-09.3

12.4. Virus Prevention: PSG 100-09.4

12.5. Firewalls: PSG 100-09.5

12.6. Data Encryption: PSG 100-09.6

12.7. Remote Access: PSG 100-09.7

12.8. Passwords: PSG 100-09.8

12.9. Servers: PSG 100-09.9

12.10. Physical Access: PSG 100-09.10

12.11. Traffic Restrictions: PSG 100-09.11

12.12. Wireless: PSG 100-09.12

12.13. Laptop: PSG 100-09.13

12.14. Disposal of Hardware: PSG 100-09.14

12.15. Application Assessment/Certification: PSG 100-09.15

1. The following document is a listing of all Enterprise Security Technical Documents.

   1.1. Web Servers: PSG 100-09.2

   1.2. Email: PSG 100-09.3

   1.3. Virus Prevention: PSG 100-09.4

   1.4. Firewalls: PSG 100-09.5

   1.5. Data Encryption: PSG 100-09.6

   1.6. Remote Access: PSG 100-09.7

   1.7. Passwords: PSG 100-09.8

   1.8. Servers: PSG 100-09.9

   1.9. Physical Access: PSG 100-09.10

   1.10. Traffic Restrictions: PSG 100-09.11

   1.11. Wireless: PSG 100-09.12

   1.12. Laptop: PSG 100-09.13

   1.13. Disposal of Hardware: PSG 100-09.14

   1.14. Application Assessment/Certification: PSG 100-09.15

1. If an Agency maintains a web server that resides on the State network and needs it to be mapped through the firewall so that it is accessible from the Internet, there are several security requirements that must be met. These include:

   1.1. ITS will perform network address translation (NAT) to convert the private IP address to a public IP address so the server may be accessible from the Internet. However, ITS will only open up ports HTTP and/or HTTPS for this sever.

   1.2. Agency is required to "harden" these servers. Hardening these servers includes: regularly installing all service packs, patches, and updates after appropriate integration testing; disabling all unnecessary services, devices, and accounts; enabling appropriate logging and routine log activity review procedures; and establishing adequate access and control mechanisms.

   1.3. Physical Location: ITS will permit this web server to be physically located in the Agency local network. However, the agency is required to place that Internet-accessible web server on a "de-militarized zone" or DMZ segment behind a firewall. As an alternative, ITS recommends that the Agency consider moving their web services within the ITS DMZ located within the State Computer Center. Although the ITS DMZ is within a secure, restricted area, agencies' locating servers there will still have 24/7 access to their equipment.

1. For the purpose of security and limiting spam into the network, 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 relay. The inside mail relay forwards the mail on to the appropriate mail server. Also, all mail going out passes through the inside mail relay first and then is "relayed" to the outside mail relay before being forwarded to the Internet. For this reason, agencies must adhere to the following guidelines in regard to incoming/outgoing mail:

   1.1. No direct SMTP to and/or from the Internet. Agencies must utilize the ITS maintained mail relays for mail traveling in both directions.

   1.2. No POP or IMAP from Internet to mail servers inside State network. Agencies must utilize a secure web interface (HTTPS) to access this mail.

   1.3. 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.

2. Agencies must establish policies to help employees use email properly, to reduce the risk of intentional or inadvertent misuse, and to assure that official records transferred via electronic mail are properly handled. Principle priorities are:

   2.1. Email communications must not be unethical, fraudulent, harassing, obscene, be perceived as a conflict of interest, or contain sensitive information.

   2.2. File attachments sent via e-mail must be scanned using current anti-virus software prior to sending the transmission. Any file attachment that is received should be scanned prior to opening the file.

   2.3. Users must not allow anyone else to send email using their accounts.

   2.4. Email must be used to conduct official business only.

# Mississippi Department of Information Technology Services

| | | |
|---|---|---|
| **Doc Ref Number:** | PSG 100-09.4 | **Published by:** ISD |
| **Document Type:** | Enterprise | **Page:** 1 of 1 |
| **Effective Date:** | September 21, 2009 | **Revision Date:** |
| **Title:** | **Enterprise Security: Virus Prevention** | |

1. Agency must:

   1.1. Maintain virus scanning software on all servers and workstations.

   1.2. Keep virus signature files 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 at higher risk.

   1.3. Instruct end-users of the danger of opening emailed file attachments they were not already expecting to receive.

   1.4. Immediately remove any infected workstation or server from the network until the virus has been cleaned.

   1.5. Maintain copies of virus-detection and eradication tools offline.

2. ITS will monitor for network activity that indicates the presence of malicious code, and upon detection will block access to the State Network for the infected workstation or server. Once the block is put in place, ITS will notify the agency contact. When the agency contact confirms that the workstation or server has been cleaned, ITS will remove the block.

# ITS Mississippi Department of Information Technology Services

| | | |
|---|---|---|
| **Doc Ref Number:** | PSG 100-09.5 | **Published by:** ISD |
| **Document Type:** | Enterprise | **Page:** 1 of 1 |
| **Effective Date:** | September 21, 2009 | **Revision Date:** |
| **Title:** | **Enterprise Security: Firewalls** | |

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.

   1.1. 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.

   1.2. Outbound connections from the State Network will be largely unrestricted. Exceptions to this include LAN protocols, ICMP, and ports known for propagating malicious code.

2. Agencies are required to implement firewalls at the perimeter of their networks, to secure their 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.

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

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

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

2. If an agency Internet-facing server gathers or transmits sensitive data from customers the application must use, at minimum, SSL for the transaction. It is required that a reputable 3rd party server certificate be used for this SSL transaction. If agency security requirements for an application require client-based digital certificates, the agency must consult with ITS before implementation.

3. It is recommended agencies consider the encryption of sensitive data at any point it leaves their local trusted network. For example, if Agency A must send sensitive data to Agency B, the sensitive data must leave Agency A's local trusted network and travel a common, shared (State) network infrastructure to get to Agency B's trusted local network.

4. Agencies must encrypt sensitive data stored on any of their local servers. Agencies must also ensure that any sensitive data on servers located offsite is properly encrypted.

1. The following policies address connectivity into the State network from any entity that resides outside the trusted State network (ie. outside State border firewall). This includes third party entities' connectivity into the State network via the public Internet, as well as, private circuits.

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

   1.2. Split-tunneling MUST be disabled on any device (firewall, VPN Concentrator, etc.) used to terminate VPNs behind the State's firewall and/or the agency's firewall or any remote device/software that utilizes the VPN.

      1.2.1. 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.

      1.2.2. 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.

   1.3. VPNs may be client-based or LAN-to-LAN-based.

      1.3.1. Client-based VPNs are VPNs in which a 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).

      1.3.2. 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.

1.4. In implementing VPNs, tunnels must be limited with access-restrictions that are granular enough to restrict traffic to both IP addresses and specific TCP/UDP ports. The list of addresses and ports allowed must be pared down to only what is necessary for the applications used by the remote users.

1.5. ITS maintains Cisco VPN termination devices to establish client-based and LAN-to-LAN VPNs for access to resources on the State Network.

1.5.1. Direct telnet access via TN3270 from the Internet to the State Data Center is not permitted.

1.5.2. All LAN-to-LAN VPNs will be implemented using the IPSec protocol.

1.5.3. Any third party entity that needs a connection to the State Network must provide and maintain compatible industry-standard IPSec-capable VPN hardware/software solution at their end of the connection. VPN must be addressed using public IP addresses registered to that entity, including the peer address and any networks behind the third party VPN device 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.

1.5.4. Client-based VPNs may be implemented with IPSec or SSL.

1.6. 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.

1.7. 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.

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

2. Agency Administration of Password Policy

   2.1. Automated password input must not be allowed, except for simplified/single sign on systems that have been approved by ITS.

   2.2. Passwords must not be stored in clear text on hard drives or any other electronic media. If stored on electronic media, passwords must be encrypted.

   2.3. Where possible and practical, access to password-protected systems must be timed out after an inactivity period of thirty (30) minutes or less or as required by law, if the inactivity period is shorter than thirty (30) minutes.

   2.4. Passwords for administrative accounts must be treated with a higher level of security including, changing admin accounts every (30) days, immediately revoking access when administrators leave or are terminated, minimizing the number of staff with admin accounts and access, and consideration of two-factor authentication for administrative accounts.

   2.5. Third-party support accounts must be disabled or deleted when not in use.

   2.6. Promptly remove user accounts for staff no longer employed.

3. Agencies must enforce the following guidelines for user passwords:

   3.1. Passwords must contain at least 8 nonblank characters.

   3.2. Passwords must contain a combination of letters (preferably a mixture of upper and lowercase letters), numbers, and at least one special character within the first seven positions. Examples of special characters include #, $, _, and @.

   3.3. Passwords must not contain the user ID.

   3.4. 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.

3.5. Passwords must not include common words from an English dictionary or foreign-language dictionary.

3.6. Passwords must not contain commonly used proper names, including the name of any fictional character or place.

3.7. Passwords must not contain any simple pattern of letters or numbers such as "qwertyxx" or "xyz123xx."

3.8. Passwords must not be trivial, predictable or obvious.

4. Agencies must instruct their users to follow these guidelines for the purpose of protecting passwords:

4.1. Passwords must not be disclosed to anyone except in emergency circumstances or when there is an overriding operational necessity.

4.2. Passwords must not be left in a location accessible to others.

4.3. Passwords must never be written down.

4.4. Passwords must not be sent in clear text over the network. Secure Shell (SSH) and HTTPS must replace Telnet and HTTP for authentication.

4.5. Passwords must be unique per user.

4.6. Passwords must be changed at least every 6 months and never reused.

4.7. Default passwords must be changed.

4.8. Passwords must be required on all user accounts.

4.9. Passwords suspected to be stolen or cracked must be changed immediately and notification must be given to the user's supervisor and system administrator.

5. For users that have access to highly 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.

5.1. Possible authentication factors are generally classified into three categories:

5.1.1. Something the user has such as a Smart card, security token, or USB token;

5.1.2. Something the user knows such as a password, pass phrase, or personal identification number (PIN);

5.1.3. Something the user is or does such as a fingerprint, retinal pattern, DNA sequence or other biometric identifier.

6. ITS Mainframe Passwords Requirements

6.1. The current mainframe security software, RACF, requires passwords to be an eight (8) character alphanumeric password.

6.2. Passwords are not case sensitive.

6.3. Passwords must not contain the user ID.

6.4. 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.

6.5. When changing a password, none of the six previous passwords will be accepted.

6.6. The system default for the password change interval is sixty (60) days; however, some state agencies have requested the password interval be set to a number less than 60 days.

6.7. After two (2) unsuccessful attempts to logon, the user-id gets revoked and must be reset by the ITS Service Desk.

1. Agencies must configure all servers to reflect their security requirements and reconfigure them as their requirements change.

   1.1. Agencies are required to "harden" their servers. Hardening these servers includes: following proper configuration management protocol, regularly installing all service packs, patches, and updates after appropriate integration testing; disabling all unnecessary services, devices, and accounts; enabling appropriate logging and routine log activity review procedures; implementing adequate virus protection; and establishing adequate access and control mechanisms.

   1.2. Proper physical location of the server must be considered. Refer to Technical Document PSG 100-09.10 Physical Access.

1. A majority of security violations, vandalism, and even accidental acts that lead to disruption of services can be attributed to deficiencies in physical security. The guidelines below must be considered in order to maintain adequate physical security for each agency.

    1.1. Locate computer equipment in inconspicuous places without signs, maps, and external references.

    1.2. Locate computer equipment away from windows or any other place that allows easy access by outside individuals.

    1.3. Locate computer equipment in places that can be environmentally controlled.

    1.4. Locate computer equipment away from heavy traffic areas.

    1.5. Locate computer equipment in rooms that can be physically secured.

    1.6. Locate computer equipment in areas to minimize the likelihood of accidents. For example, do not place equipment in rooms that contain overhead water pipes or in rooms next to large mechanical systems.

    1.7. Locate computer equipment in buildings that are of less risk for potential disaster situations (i.e. buildings located in flood zones, near railroad tracks, or remote to fire departments).

2. Agencies must adhere to the following access control guidelines:

    2.1. Larger computer installations must be equipped with an access control system, normally a card access system. Access then can be limited to specific individuals at specific times and dates. Dates and times can be recorded to track access. Specific procedures must be in place to control the assignment and authorization level of access to facilities and to terminate access should access requirements change. Other than the access control system, larger installations should:

        2.1.1. 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).

2.1.2. Use cameras to record activity in and around computer installation.

2.1.3. Archive access system and video data for a period of one year.

2.1.4. Restrict visitors in the computer facilities. Visitors that are allowed access must sign in and must be accompanied by an authorized staff member.

2.2. Smaller computer installations, especially those that contain critical servers, must be kept in locked rooms. The number of individuals with access to the room must be limited.

2.3. Any PC that is connected to an agency LAN or to the State Network must be placed in a room that can be locked after hours. Any PC that is left unattended during the day must be logged out or locked when there is no activity (keyboard or mouse) for an extended period of time.

2.4. Any PC that contains critical information should be located in a room that can be locked.

2.5. Wiring closets should be locked at all times.

2.6. Rooms or closets that contain State Network routers or switches must be locked at all times. This includes remote offices.

2.7. Agencies should insure that all laptops are stored in secure locations and that there is a strict checkout procedure for issuing laptops to staff members.

3. Agencies must adhere to the following Environmental and Electrical guidelines:

3.1. Computer facilities must have fire protection. Larger facilities should have a pre-action fire suppression system installed. All facilities must have strategically placed hand held fire extinguishers. Fire extinguishers must be inspected yearly by the Fire Department.

3.2. All facilities must deploy smoke and heat detectors.

3.3. Flammable or toxic materials must not be stored near computer equipment.

3.4. Larger installations must deploy water detectors.

3.5. Electrical systems for critical computer equipment must include Uninterrupted Power Systems (UPS). A generator should be considered for this critical equipment also. Surge protectors should be considered for equipment sensitive to power fluctuations.

3.6. Larger facilities must ensure that adequate room temperature and humidity is maintained to the specifications of the hardware vendor. Redundancy must be built into any HVAC system. Any system should include facilities for monitoring the environment and sounding alarms when thresholds exceed normal limits.

3.7. Areas housing environmental or electrical systems critical to computer facilities should be protected by access control systems and monitored by security cameras.

4. Agencies should adhere to the following miscellaneous physical security guidelines:

4.1. 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.

4.2. Backup and recovery materials (tapes, manuals, etc.) must be kept at a site that meets stringent physical security measures. This site should be accessible 24/7/365.

# Mississippi Department of Information Technology Services

| | | |
|---|---|---|
| **Doc Ref Number:** | PSG 100-09.11 | **Published by:** ISD |
| **Document Type:** | Enterprise | **Page:** 1 of 1 |
| **Effective Date:** | September 21, 2009 | **Revision Date:** |
| **Title:** | **Enterprise Security: Traffic Restrictions** | |

1. Agencies must adhere to the following non-state business traffic polices:

   1.1. 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.

   1.2. ITS has developed an Acceptable Use Policy (AUP) for its employees. This AUP defines proper use of state resources by agency users. Each agency should enact an acceptable use policy for their agency's infrastructure. ITS's AUP can be viewed at: http://www.its.ms.gov/docs/itsusepolicy.pdf

1. The purpose of this policy is to outline security and data integrity measures required for implementing and securing wireless local area networks that reside within the State of Mississippi's wide area network.

2. 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.

3. Any agency that implements a wireless network solution assumes all responsibility and will be held accountable for all unauthorized State network intrusions, loss of data/systems, and attacks attributed to their wireless network.

4. An agency should not undertake wireless deployment for any operations until it has examined and can acceptably manage and mitigate the risks to its information, system operations, and continuity of essential operations.

   4.1. Maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems.

   4.2. Agencies must assess risks more frequently and test and evaluate system security controls when wireless technologies are deployed.

5. Before implementing a wireless network, agencies must notify the ITS Information Security Division of their intent to do so. If the agency has previously implemented a wireless solution and not notified ITS, agencies must notify the ITS Information Security Division of the existing deployment.

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

   6.1. The placement of wireless LAN Access Points (WAP) must be strategically located to minimize the interception of wireless signals by unauthorized individuals or outside the intended coverage area. WAPs should be mounted above ceiling tiles, out of plain site, or otherwise publicly inaccessible and not visible to unauthorized persons. The range of WAPs must also be tested to ensure that signals are not being transmitted outside the intended coverage area.

6.2. All WAP installations must use encryption. WPA Version 2 with AES is the minimal level of acceptable encryption. WEP and WPA (version1) are not permitted.

6.3. WPA Version 2 may be deployed in either "PSK mode" or "Enterprise mode" with specific requirements for each mode.

6.3.1. PSK mode deployment requirements

6.3.1.1. The "key" or "pass-phrase" should be known and kept securely by as few personnel as possible.

6.3.1.2. The "key" or "pass-phrase" should be changed regularly. Regularly is defined as every six months for minimum standards, however, it is recommended to be changed every three months.

6.3.1.3. Very strong password creation practices should be followed when creating WPA-PSK passwords. At minimum, 16 characters with alpha-numeric, upper case, lower case and special characters should be used. Words easily found in a dictionary or common phrases must not be used.

6.3.1.4. May be used when remote clients are not mobile and the network administrator can easily control and change the passwords regularly.

6.3.2. Enterprise mode deployment requirements:

6.3.2.1. Recommended as most secure method for protecting wireless data.

6.3.2.2. This option requires the use of an 802.1x client supplicant software and a Radius server.

6.4. 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. Also, the beacon interval on the WAP must be set to the longest interval possible. Where applicable, the new settings should be not easily discernable or provide clues to the location, agency, or data / system description.

6.5. WAPs must be connected to a switch and not a hub.

6.6. Physical security of WAPs must be maintained to protect the WAP from theft or access to the data port.

6.7. The SSID should not openly identify the LAN or its purpose, and should be constructed as securely as a password. Open broadcasting of the SSID must be disabled.

6.8. Agencies should consider the use of VPNs for specific users or network segments that need to transmit sensitive and confidential information or data for an added measure of security on top of the WPA (version 2) protocol.

6.9. Software and firmware updates from the wireless manufacturer should be applied to the WAP and affected wireless cards as soon as possible after release to keep the security updated.

6.10. Additionally, the following wireless security best practices are recommended for deployment and operation of a wireless network.

6.10.1. 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.

6.10.2. Dynamic Host Configuration Protocol (DHCP) on wireless networks is strongly discouraged.

6.10.3. WAP configuration settings should be periodically assessed to ensure security mechanisms are being properly implemented. There are various tools on the market that can be used for capturing WAP configurations.

6.10.4. Periodic security reviews should be conducted to ensure that changes to the wireless LAN have not exposed the network to intruders. In addition, the network should be periodically scanned to detect unauthorized devices.

6.10.5. 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.

1. Agencies must adhere to the following policies on laptop physical security for laptops with sensitive data. It is recommended that agencies consider enforcing some or all of these policies for any laptop regardless of data content.

    1.1. Secure laptops with a cable lock whenever it is unattended in any location other than your office or home.

    1.2. Register computer serial #/model # with mfg, & store information separately.

    1.3. Establish hard drive and/or BIOS password standards for the agency or each department of the agency. Enable these features on each laptop and configure a password per this standard. A hard drive password is preferred as it "locks" the hard drive preventing it from being accesses by physically installing it in a similar computer.

    1.4. Apply a tamper resistant asset tag or engrave the machine to aid authorities in recovery.

    1.5. Use a non-descript carry case. Place the laptop in a padded sleeve inside a backpack for example.

    1.6. While traveling, never leave a laptop unattended in a public place.

    1.7. Consider software that aids in tracking and recovery of the laptop if lost or stolen.

    1.8. If a laptop is lost or stolen, report it immediately.

2. Agencies must adhere to the following policies on laptop operating system security:

    2.1. If leaving a laptop unattended, log out or turn machine off.

    2.2. Use the latest version of the operating system. Enable auto updates from the agency network and the Internet when not at the office.

    2.3. Disable boot-up capabilities of other drives. Disabling the secondary boot drive sequence hinders the ability to access the system from a secondary drive.

    2.4. Rename the Administrator Account. When renaming, don't use the word "Admin" in its name.

2.5. Prevent the last user name from displaying in the login dialog box.

2.6. Ensure only one active connected network interface is enabled at a time. For example, if WiFi is enabled, then other access methods are disabled.

2.7. On laptops with sensitive data, prohibit users from downloading third party software and applications or enabling unauthorized protocols or services.

3. Agencies must adhere to the following policies on laptop network security:

3.1. Install and regularly update an Antivirus product. Enable real time protection.

3.2. Install host-based Adware and Spyware utilities.

3.3. Install and regularly update a host-based firewall.

3.4. Use client patch management software to receive the latest fixes to OS and software.

4. Agencies must adhere to the following policies for protecting laptop data:

4.1. Back up and synchronize your files on a regular basis.

4.2. Consider using offline storage products when traveling. USB drives, RW CD's, or external hard drives provide a good back up should your laptop be unavailable. These drives should be encrypted as well. Only agency storage devices should be used. Do not use personal storage devices (ie. personal USB drive).

4.3. Use privacy screens when using your laptop in public places

4.4. Use system encryption tools for encrypting individual files and folders. The backup of data should be encrypted as well.

4.5. For the most complete protection of data on the computer, install whole disk encryption.

4.6. For machines with sensitive data, consider installing disk wiping technology that remotely wipes the hard drive clean in the event of loss or theft.

1. Before disposal, agencies must determine if the hardware contains any sensitive data

   1.1. Agencies must sanitize or remove all data and software from the device.

   1.2. Simply erasing and reformatting hard drives is not a permissible method way of sanitizing magnetic media before disposal.

2. Before disposing of old hardware, agencies must use one of the following methods of sanitizing the hardware device:

   2.1. Overwriting – This method should be used when the technology still contains usefulness and can be used elsewhere by a third party.

      2.1.1. Agencies may sanitize magnetic media (ie. hard disk) by an overwriting process whereby a software utility writes a combination of 0s and 1s over each location on the hard drive multiple times.

      2.1.2. This process obscures the previous information, rendering the data unreadable. Agencies must overwrite the disk three times prior to disposal or reuse.

   2.2. Physical Destruction – This method should be used when the technology contains no usefulness and will be permanently disposed of (ie. thrown in dumpster) or if the magnetic media contains highly sensitive data.

      2.2.1. In this case, the agency should perform a complete and permanent elimination of data and media device.

      2.2.2. Physical destruction is done by shredding the entire drive or the drives platters. At minimum the platters must be badly warped or distorted, rendering the drive or any of its components inoperable.

      2.2.3. This can generally be achieved by drilling the drive in several locations perpendicular to the platters and penetrating completely through from top to bottom.

2.2.4. Hammering or crushing is equally effective but more labor intensive.

2.2.5. Simply destroying the logic section of the drive without damaging the platters is insufficient. If a third party vendor is utilized, a certificate of destruction must be obtained.

2.3. Degaussing - This method should be used when the technology contains no usefulness and will be permanently disposed of (ie. thrown in dumpster) or if the magnetic media contains highly sensitive data.

2.3.1. Agencies may utilize a degaussing process to erase the magnetic media but it requires specialized equipment designed and approved for the type of media being purged.

1. Agencies must test all new applications using a security verification process that ensures key application security and privacy dependencies are met and new security relevant code in the application and supporting infrastructure services are reviewed for common errors that can compromise the integrity of the production environment when the application is deployed.

    1.1. Agencies can contract with a third party to perform the assessments, perform them internally, or implement assessment software. Regardless of the method of assessment, the following vulnerabilities must be assessed, at minimum.

        1.1.1. Un-validated input

        1.1.2. Broken access control

        1.1.3. Broken authentication and session management

        1.1.4. Injection flaws

        1.1.5. Improper error handling

        1.1.6. Insecure configuration management

        1.1.7. Insecure storage

2. Prior to deployment, agencies must submit in writing to the ITS, a summary of this security verification testing as proof the proposed system has been tested for security and privacy vulnerabilities.

3. The application security assessment must be repeated at least annually and must be considered at any time the application is modified or updated.

    3.1. Each repeated assessment must also be submitted to ITS.