STATE OF ALABAMA

Information Technology Standard

STANDARD 662S2-03: CLIENT SYSTEMS SECURITY

Client systems include workstations, personal computers, laptops, and other portable devices on which users run applications. Client systems will connect to, communicate with, and share data with other systems on a network.

Hardening client systems results in a substantial reduction in vulnerability exposure and improves the effectiveness of the enterprise security program. Proper security and configuration of client devices will reduce the risk of physical theft, the introduction of malicious logic, and the likelihood of data loss, and the implementation of secure connectivity mechanisms will protect the State network and reduce the risk of unauthorized access.

OBJECTIVE

Establish safeguards for the security of client devices including (but not limited to) desktops, laptops, and other portable computing and data storage devices.

SCOPE

These requirements apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

CONFIGURATION CONTROLS

Prior to processing State information on any client device the Agency Information Security Officer (ISO) shall ensure the device (including associated peripheral devices, operating system, applications, network connection methods, and services) complies with applicable state standards and agency requirements.

System and network administrator personnel shall establish written procedures and a testing methodology to ensure that all devices are appropriately configured before granting access to State network resources.

OPERATING SYSTEM:

The CIS Security Benchmarks Division develops and distributes Security Configuration Benchmarks describing consensus best practices for the secure configuration of IT systems. Configuring systems in compliance with these Benchmarks has been shown to eliminate 80-95% of known security vulnerabilities. Download the applicable operating system Security Benchmark from:

http://benchmarks.cisecurity.org/en-us/?route=downloads.browse.category.benchmarks.os

Ensure the operating system is secured in accordance with the applicable client operating system Security Benchmark. Document any difference between the benchmark settings and the final system configuration.

Operating systems shall be maintained at a service pack level supported by the vendor with new security updates. Operating systems (and application software) that are unsupported will not receive security updates making them vulnerable and subject to exploitation. Unsupported systems may be isolated from other network resources until brought up to date.

Ensure the latest operating system and third-party application patches are installed.

ACCESS CONTROLS:

All client devices shall be protected by authenticated logon using a PIN, password, or passphrase. Users shall not bypass device authentication.

Use a password protected screensaver to lock the device during periods of inactivity.

Handheld devices shall utilize an inactivity timeout whereby the user must reenter their user PIN/password to unlock the device.

Set the device inactivity timeout setting to no more than 15 minutes.

ADDITIONAL CONFIGURATION CONTROLS FOR MOBILE DEVICES:

In addition to the above configuration controls, mobile client devices shall also comply with the following security controls:

Firewall:

Use a host-based firewall or intrusion prevention software to deter intruders and malicious logic from entering the system via an un-trusted connection (then subsequently entering the State network when the system is returned to the local network).

Never use free or trial-use host-based firewalls as much of the functionality required to adequately protect or manage the granularity of the firewall rules is non-existent.

Networking:

Secure or disable file and printer sharing.

Disable peer-to-peer (ad-hoc) networking capabilities, if so equipped, to prevent inadvertent peer-to-peer communications.

Encryption:

Utilize full-disk encryption (FDE) to protect all data on State-owned laptops and encryption-capable portable devices.

GENERAL SECURITY REQUIREMENTS

The following requirements are based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-46: Guide to Enterprise Telework and Remote Access Security, and other best practices. These requirements apply to portable devices such as laptops and handheld devices.

PHYSICAL SAFEGUARDS:

Secure portable devices (especially laptops) using a cable lock or alarm. Attach the locking cable to an immovable or unbreakable object. If leaving a device out overnight, lock the entrance(s) to the room. If the room cannot be locked then secure the device in a locked cabinet or safe.

Eject access card devices and peripheral storage devices from the host system and secure them separately.

Never leave a portable device in view in a vehicle; do not leave devices in a vehicle overnight.

According to the FBI, 97% of unmarked computers are never recovered. Marking the device may increase the chances of having it returned and may also deter casual thieves. Asset tag or engrave the device by permanently marking (or engraving) the outer case or an accessible internal area with the agency name, address, and phone number.

Include a “Return to Sender” text file on any portable devices. This will not deter theft, but it may increase the chances of the device being returned in the event it is found, turned-in for maintenance, or retrieved in the course of an investigation.

For laptops, use a non-descript carrying case rather than a laptop case displaying the manufacturer's logo. Consider using a form-fitting padded sleeve for the laptop and carrying it in a backpack, courier bag, briefcase, or other common non-descript carrying case. Close and lock the zippers of the case so no one can simply reach in and remove the laptop.

Use privacy screens in public facilities or open, high-traffic environments to prevent “shoulder-surfing” when on-screen data needs to be kept private.

LOST DEVICES:

Users shall immediately report the loss of any computing or data storage device (including personally-owned devices if used to connect to State networks or store State data) to their manager, IT Manager, or Information Security Officer (ISO).

If possible, Administrators shall perform a remote data wipe to clear the device’s memory.

Because network administrative accounts may have been cached on the device while it was connected to the host network, the System Administrator must change any local network administrative authenticators that may have been used on the lost device.

Recovered devices shall be treated as compromised. Do not connect a previously lost device to any operational network or system until the device has been properly sanitized. There is a significant risk in transferring any user or operational data from the system since there are numerous methods to install and hide malicious code.

TRAVEL:

Public hotspots and wireless LANs (WLAN) installed at airports, hotels, and other establishments present high security risks. Wireless encryption and access controls on the laptop often need to be disabled before connecting to a public WLAN, thus, any information exchanged is sent unencrypted. Furthermore the device may be subject to probes and scanning from other clients connected to the WLAN, therefore, the following protective measures shall be followed:

- Do not use a public WLAN unless it is absolutely necessary
- Use a VPN (otherwise all messages can be intercepted)
- Use a personal firewall and ensure its settings are set for maximum protection
- Upon leaving the WLAN, immediately restore all security settings and scan the device for viruses and other malware

The longer a system remains disconnected from its supporting infrastructure, the greater the risks of the system being compromised. Therefore, when the risks of un-patched systems are greater than the threats posed by elevated user privileges, consider granting users privileged-level access so they are able to manage and update their own system during extended or remote absences.

Do not download software or applications while on travel unless from a trusted source over a secure channel.

Any device that has been on travel or was connected to an external or un-trusted network shall be checked for compliance with security policies prior to gaining access to State network resources.

REMOTE ACCESS CONNECTIONS

Utilize the State Virtual Private Network (VPN) to remotely connect to the State network or direct dial connection to State-provided Remote Access Servers (VPN connectivity is the preferred connection method). VPN use and configuration shall comply with State VPN standards.

Secure Sockets Layer (SSL) access to e-mail (e.g., Outlook Web Access) or data access using application layer security through a “thin client” (e.g., CITRIX) are acceptable alternatives to VPN access (unless access to the state backbone is a requirement).

Remote access connectivity shall comply with applicable state policy and standards.

Ensure wired network interfaces (e.g., Ethernet) are disconnected or otherwise disabled when wireless network connections are being used. Similarly, disable the wireless function when connected to a wired network. This ensures the device cannot be accidentally or intentionally used as a bridging or routing device between two or more networks.

PORTABLE DEVICE SECURITY

These requirements apply to portable devices that are configured to send/receive State of Alabama e-mail or connect to State network applications and/or data and to the system components required to support such devices (including):

- Wireless handheld device (e.g., PDA, Smartphone)
- Software installed on the handheld device by the device manufacturer or wireless carrier (e.g. operating system, internet browser, productivity applications)
- Wireless e-mail product client and server software
- IT Security Policy Management Server
- Gateway Server, located with the IT Security Policy Management Server, providing connection between the wireless handheld device and enterprise network services

Requirements apply to all brands of portable device (including but not limited to Blackberry, Treo, iPhone, and Palm devices).

GENERAL REQUIREMENTS:

E-mail redirection (push) from the Exchange Server to a wireless device shall be State-controlled via a centrally managed server. Desktop or Internet controlled e-mail redirection is not authorized.

Disable peer-to-peer (ad-hoc) networking capabilities, if so equipped, to prevent inadvertent peer-to-peer communications.

DEVICE AUTHORIZATION:

Any individual possessing a State-provisioned portable communication device must read and sign an agreement indicating that he or she understands and will comply with the terms and conditions of use stated therein. The User shall submit annually, no later than January 31st, a completed User Declaration for each provisioned device that has been assigned to him or her. The agreement must be signed by an appropriate signing authority that represents the employing state agency of the User. The employing state agency assumes responsibility for enforcing the terms of the agreement.

Users may be further subject to any rules, regulations or policies of the user's employing agency.

The Portable Device Terms and Conditions of Use Agreement and User Declaration form may be obtained from: http://cybersecurity.alabama.gov/forms.aspx.

DEVICE REQUIREMENTS:

Hot-sync Operations:

Hot-sync management software shall use some form of access control (e.g., user password is entered before a hot-sync operation can be executed).

Wireless operations shall be disabled when a PDA is connected to the State of Alabama wired network via a hot-sync or other interface cable.

PDA's that transmit receive, store, or process State Sensitive or Confidential information shall not be synced to home or personally-owned PCs.

Device Sanitization:

Sanitize PDA devices prior to disposal or reuse; when turning devices in for upgrade, repair or service termination; or upon changes in employment (transfer, resignation, retirement, termination, etc.).

The system administrator shall have the capability to remotely transmit a “data wipe” (hard reset) command to the handheld device. The “Data Wipe” function will erase all data (operating system, applications, and data) stored in user addressable memory on the handheld device.

PERSONALLY-OWNED DEVICES:

When used to communicate with State systems personally-owned portable devices shall comply with the requirements stated in this and other applicable state standards.

Technical support for personally-owned devices is the owner’s responsibility. State support personnel will perform only limited support such as provisioning the device so it can receive State e-mail and connect to State network resources and limited diagnostic activities to establish whether a problem is hardware, software, or security incident related.

ADDITIONAL INFORMATION:

Information Technology Policy 662: Systems Security
http://cybersecurity.alabama.gov/documents/Policy_662_Systems_Security.pdf

Information Technology Procedure 662P1: Portable Device Authorization
http://cybersecurity.alabama.gov/documents/Procedure_662P1_Portable_Device_Authorization.pdf

Information Technology Policy 623: Authentication
http://cybersecurity.alabama.gov/documents/Policy_623_Authentication.pdf

Information Technology Policy 622: Remote Access
http://cybersecurity.alabama.gov/documents/Policy_622_Remote_Access.pdf

Information Technology Standard 622S1: Virtual Private Networks
http://cybersecurity.alabama.gov/documents/Standard_622S1_Virtual_Private_Networks.pdf

Information Technology Standard 643S2: Wireless Clients
http://cybersecurity.alabama.gov/documents/Standard_643S2_Wireless_Clients.pdf

Information Technology Policy 683: Encryption
http://cybersecurity.alabama.gov/documents/Policy_683_Encryption.pdf

Information Technology Dictionary
http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
662S2-00	09/01/2011	This document consolidates and replaces Standards 660-02S1: Laptop Security and 660-02S2: PDA Security.
662S2-01	07/26/2012	Added Device Authorization to Portable Device Security; added reference to Procedure 662P1: Portable Device Authorization.
662S2-02	09/21/2012	Replaced NSA Security Guide link with CIS Security Benchmark link.
662S2-03	08/01/2013	Added requirement to use vendor-supported operating systems and software.