

APPENDIX F: STATE OF ALABAMA SECURITY GUIDELINES

***** DRAFT *****



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Commitment to Information Security

Policy Number: 600-SU01	Version: DRAFT	Effective Date:
-------------------------	----------------	-----------------

Notice: The policies set out in this appendix are draft information security policies from the Department of Finance Information Services Division. For the purpose of this procurement, however, the policies are considered final and fully in effect. Vendor proposals must adhere to these policies or be subject to point deductions during proposal evaluation.

Purpose

This policy is intended to communicate to all State of Alabama employees the commitment to information security and to define the individual user's responsibility for ensuring information security policies, procedures, and standards are adhered to and enforced. This policy, applicable laws, and other relevant State, agency, and system policies, govern use of electronic communications resources provided by the Information Services Division (ISD) of the Department of Finance. ISD, as the State's central provider of data network services, has a significant responsibility to its customers to conduct business in a secure and reliable manner.

Scope

This ISD Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information systems.

Policy

State employees, contractors, vendors, and business partners providing or utilizing information technology services for the State of Alabama will abide by and follow ISD information security policies and procedures and adhere to all security standards.

Each user – employee, contractor, vendor, and business partner (see Definition) – is responsible for reading, understanding, and complying with ISD information security policies.

Users will sign an agreement indicating that they have read the security policies, that they understand what is required of them, that they are committed to comply with those policies and the supporting procedures and standards, and that if they fail to comply, they may be subject to disciplinary action.

Enforcement

Authority

The Code of Alabama 1975 (Section 16-61D-1), created the Information Services Division of the Department of Finance, and with Executive Order Number 20 granted it the authority to establish all necessary policies and procedures to carry out the requirements of that order.

Reporting

Users will report any security-related issues to their immediate supervisor, manager, or as outlined in the applicable information security policy, standard, or procedure.

Non-compliance

Employee conduct or behavior while using any State-managed information system must comply with ISD information security policies. Violation can result in disciplinary action up to and including termination. Conduct or communications which violate State or Federal laws will not only be grounds for immediate termination, but may also subject the employee to criminal prosecution. Suspected violators of any laws, including copyright laws and FCC regulations, involving information services provided by the State of Alabama will be reported to the appropriate agency head and/or the Attorney General of Alabama for investigation and appropriate legal action. Some policy non-compliances may be punishable under The Code of Alabama 1975 (Section 13A-8-100), Alabama Computer Crime Act. Such cases will be referred to the appropriate authorities. Other policy non-compliances by users shall be handled in accordance with the applicable disciplinary guidelines established by the user's agency. ISD will determine on a case-by-case basis when policy non-compliance is sufficient grounds to deny the user access to information services.

Definitions

Policy: A document outlining specific requirements or rules that must be met. Policies are usually point-specific, covering a single area. For example, the Acceptable Use Policy covers the rules and regulations for appropriate use of the computing facilities.

Procedure: A set of instructions or methods for performing a specific task or function. One or more procedures may support the implementation of a security policy.

Standard: A collection of system-specific or procedural-specific requirements that must be met by everyone. For example, a standard might describe how to harden a Windows NT workstation for placement on an external network. Users must follow this standard exactly if they wish to install a Windows NT workstation on an external network segment.

User: Any State of Alabama employee, contractor, vendor, or business partner who utilizes any State-managed information systems resources including but not limited to hardware items, software, data, or access to networks.

Additional Information

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Security Awareness & Training		
Policy Number: 600-SU02	Version: DRAFT	Effective Date:

Purpose

A key element in a successful information security program is user education and awareness. Security across multiple hardware and software platforms requires security-aware users as well as a well-trained technical staff. The purpose of this policy is to ensure all employees receive appropriate information security training and to ensure increased awareness of the need for information security and compliance with information security policies and privacy regulations.

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information systems.

Policy

All users shall be briefed on information security policies, standards, and procedures affecting them at the time of employee orientation. All users shall be required to read and sign an agreement indicating they will comply with ISD information security policies, standards, and procedures.

Information systems support personnel, system administrators, and security managers shall receive on-going security training appropriate to their duties and responsibilities.

Information security shall be emphasized through information security awareness programs, education, and other reminders (such as posted notices or emailed messages). Such programs shall be made available to all personnel.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Additional Information

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release

ALABAMA

STATE OF ALABAMA GOVERNMENT INFORMATION

Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Physical Security		
Policy Number: 600-SU03	Version: DRAFT	Effective Date: [Date]

Purpose

This policy communicates the essential aspects of physical security of computing equipment and data that must be practiced by all computer users to ensure the safeguard of State of Alabama computing and intellectual property.

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information systems.

Policy

All computers, network equipment, and data will be properly secured to prevent unauthorized physical access.

Users shall ensure their personal computers are properly secured when unattended by using password-protected screen savers (for short periods of inactivity - less than one hour) or logging off the network (for longer periods of inactivity - more than one hour).

If personal computers are installed in public areas, they must be secured with an appropriate physical security device such as a lockdown mechanism.

Servers and other communications equipment shall be placed in secured and environmentally appropriate rooms with controlled access. Access shall be restricted to authorized-personnel only.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Data: A representation of information, knowledge, facts, concepts, or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed, or has been processed in a computer system or computer network, and should be classified as intellectual property, and may be in any form, including computer printouts, magnetic storage media, punched cards, or stored internally in the memory of the computer. [Alabama Computer Crime Act (Acts 1985, No. 85-383)]

Intellectual Property: Data, including computer program. [Alabama Computer Crime Act (Acts 1985, No. 85-383)]

Additional Information

Additional policies on physical security (pertaining primarily to System Administrators) are found in ISD Information Security Policy 600-SA08, Asset Protection.

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Network Access		
Policy Number: 600-SU04	Version: DRAFT	Effective Date:

Purpose

The purpose of this policy is to ensure all users are granted only the access required by job function and that all requests for access are reviewed by and approved by appropriate supervisory personnel.

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information systems.

Policy

Every user of computerized information shall have a network access account. A unique user identifier and authentication mechanism (e.g., password) shall be assigned so all activities on the network can be traced to a specific user. Every user, when signing-on, will be required to provide his or her user ID and authentication in order to gain access to the network. Identification and authentication is required each time the user signs on, and multiple levels of authentication may be used for multiple system access.

Access to the network will be requested and approved by a department manager or supervisor. Access authorization shall be consistent with the level of access required for the user to perform their assigned responsibilities.

Temporary Access Policies

Access to hosts by vendors and service providers will be granted for specific purposes only, for a limited time frame, and all activities will be logged, recorded and supervised by a manager.

Temporary identifications may be granted if required for contractors, vendors, or external regulators. All requests for temporary access shall be made in writing and will require OIT or system owner approval.

Temporary user ID's will be valid only for an agreed upon period time, and will be disabled upon expiration.

Responsibilities of Information Services Division (ISD)

ISD shall maintain a list of all users authorized to access the system identifying the user name and unique user ID, level of authority granted, user location, the date access was granted, and the date access will terminate (or was terminated).

ISD shall monitor and review the granting and rescinding of access to the network.

ISD shall ensure all local area networks connecting to the wide area network comply with the security guidelines for identification, authentication, and authorization so as not to compromise the State Security Architecture.

ISD shall review user ID's that have had no activity for 30 days to determine their status, and will remove access to inactive accounts or when the justification is no longer valid.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Host: A computer connected to a network that provides data and services to other computers.

Network: Internet, Intranet, and Extranet services provided by ISD and the State of Alabama.

Additional Information

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Acceptable Use		
Policy Number: 600-SU05	Version: DRAFT	Effective Date:

Purpose

The purpose of this policy is to define acceptable and non-acceptable use of state-owned computer resources. Inappropriate use exposes State resources to risks including virus attacks, compromise of network systems and services, and legal issues. Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. These rules are in place to protect the employee and the State.

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information systems.

Policy

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet access, and Web browsing are the property of the State of Alabama. These systems are to be used for business purposes in serving the interests of the government, and of our clients and customers in the course of normal operations.

The data users create on State information systems remains the property of the State. Because of the need to protect the State's network, management will not guarantee the confidentiality of information stored on any network device.

For security and network maintenance purposes, authorized system administrators will periodically monitor equipment, systems, and network traffic to ensure compliance with this policy.

Personal Use

Access to commercial web sites and releasing business email addresses and other identifying electronic information onto the Internet exposes computing systems to potential compromise, therefore, the non-incident personal use of State-managed computing resources is prohibited.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual agencies may create additional guidelines concerning personal use of network systems, however, no agency policy may impose a lesser limitation on personal use than is prescribed by this policy unless an exception to this policy has been specifically granted by ISD.

In the absence of agency guidelines, employees should be guided by this policy on acceptable use, and if there is any uncertainty, employees should consult their supervisor or manager.

Unacceptable Use

The following activities are prohibited:

Under no circumstances is a user authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing State-managed resources.

Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of software products that are not appropriately licensed for use by the State (refer to ISD Policy 600-SU09, Software Use).

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, as well as copyrighted music, image files, and software.

Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. Management should be consulted prior to export of any material that is in question.

Introducing malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

Making fraudulent offers of products, items, or services originating from any user account.

Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. Disruptions include, but are not limited to, packet sniffing, ping sweeps, IP spoofing, and forging routing information for malicious purposes.

Port scanning or other security scanning without prior approval of ISD.

Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

Circumventing user authentication or security of any host, network, or account.

Interfering with or denying service to any user except in the course of assigned duties.

Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network.

Using any State-managed information system to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

Sexually explicit, offensive, or inappropriate words and/or images of any kind are not permitted on State-managed computer or communications systems.

Accessing web sites that offer online games and related information such as cheats, codes, demos, online contests, role-playing games, traditional board games, game reviews, and sites that promote game manufacturers is prohibited. Fantasy sport leagues may also be included in this category of unauthorized access.

Exceptions

Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Extranet: That part of an internal computer network which is available to outside users, for example, information services for customers.

Additional Information

See Internet Access Policy, 600-SU06, and Email Use Policy, 600-SU07, for further acceptable use requirements in these areas.

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Internet Access		
Policy Number: 600-SU06	Version: DRAFT	Effective Date:

Purpose

This document defines State policies for Internet access and extends the policy on acceptable use (Information Security Policy 600-SU05) to address certain Web browsing exclusions. It is important to understand that Internet access is purchased at great expense to the State. Use of this bandwidth for other than State business is a misuse of State resources. There is also a relevant security issue because many questionable Web sites promulgate spyware and other malicious code. It is not the State's intention to make moral judgments about specific categories of Web sites--just whether particular categories of sites are necessary for conducting State business.

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information systems.

Policy

Any agency seeking Internet access must apply in writing using the established procedures prescribed by ISD. Such application must be signed by the agency head and shall state with specificity the governmental or public purposes for which access to the Internet is sought. Access to Internet services within an agency should be limited to those employees who require such access to perform their governmental duties.

The agency head is responsible for overseeing the use of Internet services provided to his or her agency. ISD shall provide periodic reports for each agency, and the agency head shall take appropriate managerial and/or disciplinary action for inappropriate uses of Internet services by state employees or other persons accessing Internet services through that agency. Failure or refusal by an agency head to properly supervise the use of Internet services by his or her agency may result in the termination of Internet services to that agency.

Internet usage records, collected and maintain by ISD, are public records under the Alabama public records laws and will be made available to the public upon request. If an agency head determines that his or her agency's use of the Internet is an exception to the public records laws, it is his or her responsibility to so provide ISD adequate justification for this claim and to arrange appropriate safeguards for restricted records.

ISD retains the right to audit an agency's use of Internet services and shall have access to all Internet usage records maintained by the using agency.

Because Internet services are to be used only for government business, all records in these systems are by definition government records. As such, these records are subject to the provisions of state laws regarding their maintenance, access, and disposition. Employees using these services should understand that they do not enjoy any right of personal privacy.

The agency head shall ensure that each employee, agent, independent contractor, or other person utilizing Internet services provided by ISD through that agency has been advised of and understands all policies and restrictions applicable to the use of such services.

Each agency shall define and implement an acceptable Internet usage policy for its employees to facilitate the efficient and productive use of the Internet as a means to accomplish the agency's mission and program goals. Agency policies shall meet minimum requirements as stated in this policy statement.

Each agency that will provide, exchange, and access information via the Internet and/or the World Wide Web must plan and implement those services by establishing necessary procedures to ensure the security of state data resources and to facilitate the efficient and productive use of those resources.

ISD has the responsibility to ensure that Alabama's government network resources are used for State business and to ensure that the network is secure. Accordingly, ISD will block certain categories of web sites that do not relate to state business including pornographic, gambling, computer gaming sites, and peer-to-peer communications (Instant Messaging services (Yahoo, MSN, AOL, etc.) and other file swapping services – see Definitions).

Accessing web sites that offer online games and related information such as cheats, codes, demos, online contests, role-playing games, traditional board games, game reviews, and sites that promote game manufacturers is prohibited. Fantasy sport leagues may also be included in this category of unauthorized access.

Exceptions

ISD will grant restriction exceptions to any blocked sites for individuals or agencies that have a need for access in order to do their jobs. This would apply to agencies such as ABI for conducting criminal investigations or other law enforcement agencies. Contact andy.cannon@isd.alabama.gov (or by phone, 334-242-4444) to arrange an exception. Be prepared to identify the URL of the blocked site(s) that should be released and whether it should be released state wide or just for specific individuals.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Internet: A worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer.

Peer-to-peer: On the Internet, Peer-to-Peer (P2P) is a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives (e.g., Napster and Gnutella). Instant Messaging (IM) services are commonly categorized as P2P.

World Wide Web: All the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).

Additional Information

See Acceptable Use Policy, 600-SU05, and Email Use Policy, 600-SU07, for further acceptable use requirements in these areas.

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Email Use		
Policy Number: 600-SU07	Version: DRAFT	Effective Date:

Purpose

The purpose of this policy is to define acceptable and non-acceptable use of the State of Alabama email system. The policies listed herein are by no means exhaustive, but attempt to provide a framework for email activities that constitute unacceptable use.

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of all State-managed electronic mail systems.

Policy

Email systems are the property of the State of Alabama and ISD and are to be used for business purposes in serving the interests of the State, and of its clients and customers in the course of normal operations.

Users should be aware that email communications on State systems remain the property of the State. Nothing in this policy should be construed to waive any claim of privilege or confidentiality for the contents of electronic mail. The State may disclose the contents of electronic communications for any business purpose or to satisfy legal obligations.

Postings by employees from a State email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the State government of Alabama, unless posting is in the course of business duties.

Users must be cautious when opening e-mail messages received from unknown senders. Attachments may contain viruses, e-mail bombs, or Trojan horse code. If there is any doubt, deleting unsolicited messages with all attached files is the safest thing to do.

Unacceptable Use

The following activities are prohibited:

Sending or forwarding emails containing libelous, defamatory, offensive, racist or obscene remarks; promptly notify your supervisor if you receive an email of this nature

Using email for personal commercial ventures, religious or political causes, endorsement of candidates, or outside organizations

Intercepting e-mail messages not destined for you

Sending email messages using another person's email account

Disguising or attempting to disguise your identity when sending mail

Unauthorized use, forging, or attempting to forge email header information or messages

Creating or forwarding chain letters or pyramid schemes of any type

Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) except in the execution of normal government information dissemination

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam)

Providing information about, or lists of, government employees to parties outside the State.

Agency managers should create and distribute an email policy containing any additional agency-specific policies appropriate to the agency's business needs, however, agency policy shall not lessen any limitations set forth in this statewide policy.

Agencies may permit employees to use e-mail for occasional and incidental personal use or may prohibit any personal use. Agencies that permit limited personal use of e-mail should direct workers to delete any message that is not a state business record, immediately after reading the message (just as any copies of sent personal messages shall be deleted immediately after sending them).

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Spam: Unauthorized and/or unsolicited electronic mass mailings.

Additional Information

See Acceptable Use Policy, 600-SU05, and Internet Access Policy, 600-SU06, for further acceptable use requirements in these areas.

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Passwords		
Policy Number: 600-SU08	Version: DRAFT	Effective Date:

Purpose

The purpose of this policy is to define the minimum requirements for password implementation and use. Detailed password requirements can be found in applicable standards and procedures documents.

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information systems that use passwords as a method of authentication.

Policy

Every user is required to provide a secure and unique password to verify their identity to the system and to receive authorization for access to the network, applications, and data. This password must be supplied each time the user logs onto the network or logs into an application.

The use of passwords to gain access to the computer system or to secure specific files does not provide users with an expectation of privacy in the respective system or document.

Keep passwords secure and do not share accounts. Do not reveal your account password to others or allow use of your account by others (this includes family and other household members when work is being done at home). Authorized users are responsible for the security of their passwords and accounts.

Passwords must never be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover them.

Passwords shall not be written down nor placed on or near the computer where they are visible.

Passwords must never be cached. Never use the “Remember Password” feature of any application (e.g., Outlook, Outlook Express, Outlook Web Access).

All PCs, laptops and workstations shall be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or be logged off the network when the host is unattended.

Minimum Password Requirements

Users shall be required to change their passwords at least every 60 days

Passwords shall be at least six characters in length

Passwords shall not be a word found in a dictionary in any language.

Passwords shall not be names. Do not use names of actors, characters from stories or movies, names from the Bible, or names related to the user.

Passwords shall use a combination of upper and lowercase characters and numbers

Passwords shall only be stored and transmitted in an encrypted format

Passwords shall not be reused within any 12month period.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Additional Information

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Software Use		
Policy Number: 600-SU09	Version: DRAFT	Effective Date:

Purpose

The purpose of this policy is to prevent software piracy and ensure State of Alabama compliance with software license agreements. Software piracy is a Federal offense. Violations can result in both civil suit and criminal charges, fines of up to \$250,000.00 per title infringed, and possible imprisonment.

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information systems.

Policy

Software piracy is illegal and is absolutely prohibited.

Users shall not copy, download, nor install unlicensed software. Users shall install and use only those versions of software authorized and licensed to the organization. Software usage shall be in compliance with the license agreement.

State employees are not permitted to install their own copies of any software onto State-managed computer systems.

State employees are not permitted to copy software from any State-managed computer system and install it on any other computer system, including their home computers, unless specifically authorized in the software license agreement.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Software Piracy: Unauthorized use of software that includes: (1) *Softloading*; purchasing a single-user license then loading the software onto multiple computers or a server. (2) *Counterfeiting*; making, distributing, and/or selling copies of software that appear to be from an authorized source. (3) Renting software without the permission of the copyright holder. (4) Distributing and/or selling software that has been unbundled (separated) from the products with which it was intended to have been bundled. (5) Downloading copyrighted software from the Internet without permission from the copyright holder.

Additional Information

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance Information Services Division

INFORMATION SECURITY POLICY

Mobile Devices		
Policy Number: 600-SU10	Version: DRAFT	Effective Date:

Purpose

The key issue to mobile security is that, given the nature of the mobile environment, no single security solution will work. Simply extending the existing security infrastructure for mobile devices simply is not practical. Mobility has its own characteristics and, hence, security issues. Key mobile security concerns include exposure of critical information, lost or stolen devices, mobile viruses, e-mail viruses, and spam. This policy defines the requirements for securing mobile devices (i.e., client devices using the 802.11 protocol which can include a workstation, laptop, Personal Digital Assistant (PDA), Blackberry, etc.).

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed mobile information devices.

Policy

Ensure that all wireless systems are approved by the Network Manager before the system is installed or used to transfer, receive, store, or process information.

Disable the wireless function of mobile devices when connected to a wired network (otherwise, the wireless network card could serve as a bridge between a wireless hacker and the wired network).

Ensure that vendor supported, State approved, anti-virus software is installed on all wireless, handheld, or mobile devices and configured in accordance with applicable policies and kept up to date with the most recent virus definition tables.

To minimize the impact of a lost device, password-protect all mobile devices, encrypt sensitive documents on the device, and do not use automatic scripts for VPN login. The password protection feature shall not permit its bypass without zeroing all data stored on the device. Passwords shall comply with all password policies as stated in ISD Information Security Policy 600-SU08, Passwords.

Install and configure host-based firewall. Verify that host-based firewall software can be installed on all WLAN client devices prior to purchase.

Power off WLAN receivers and transmitters when not in use. Verify WLAN client device management software utility has this feature prior to purchasing. Users shall also do this prior to entering sensitive areas.

Disable recording on mobile devices used in areas where highly sensitive information is stored or processed. If the mobile device does not have the ability to disable recording then users are required to turn the device off.

Use only wireless devices that allow the disabling of peer-to-peer networking capabilities. Peer-to-peer communications, also known as ad hoc networking, bypasses network based security and allows clients to directly communicate. Disable this feature to prevent inadvertent peer-to-peer communications.

For Windows 2000 and Windows XP systems, ensure most current service pack is used. To mitigate existing vulnerabilities with the Windows Wireless Zero Configuration (WZC) service disable WZC when using Windows 2000 and verify the wireless device can operate with this service disabled, or ensure Windows XP, SP2 or greater is installed.

Users shall be aware of when they are communicating wirelessly, therefore, set default setting to WLAN NIC radio to “Off”. This setting controls the status of the wireless device’s radio upon boot up. This setting, while inconvenient, will mitigate the risk to mobile devices containing sensitive data as this will force the user to actively initiate a wireless session only when needed.

Regularly back up PDA data to a PC to prevent damage from PDA-specific viruses and worms.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

WLAN: Wireless LAN, a type of local area network that uses high frequency radio waves rather than wires to communicate.

Additional Information

ISD Information Security Policy 600-SA15, Wireless Networking

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Virus Protection		
Policy Number: 600-SA02	Version: DRAFT	Effective Date:

Purpose

This policy establishes the requirements for protecting the State of Alabama computing environment from virus infections and disruptions of services. Computer systems are subject to infections of computer viruses that can destroy information and software. There are several kinds of software that can surreptitiously breach computer and/or network security including viruses, worms, Trojan Horses, and spyware (see Definitions).

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information systems.

Policy

Approved virus protection software shall be installed on all computers used to access State of Alabama information systems resources and/or data.

Virus protection programs must provide for centralized virus pattern updates, alerting, compliance reporting, and control all settings that may render the software ineffective.

Agencies shall coordinate with ISD for approved virus protection software.

All files introduced onto computers and all incoming files from external sources, including e-mail attachments and Internet file downloads, shall be processed through a virus check.

All hosts used by the employee that are connected to the State network, whether owned by the employee or the State, shall be continually executing approved virus-scanning software with a current virus database (unless an exception to this policy has been granted by ISD).

A common method of spreading a computer virus is via email, therefore, ISD will virus-scan all inbound email. All agencies shall implement administrative procedures regarding email and virus prevention.

The following policies govern the installation and use of virus protection software:

Users shall not disable virus protection software.

Users shall scan all software, downloaded files, and e-mail attachments to prevent malicious logic installation. All portable storage media (diskettes, CDs, and USB Drives) shall be virus checked before files residing on this media are transferred or accessed.

Users should not open email attachments from individuals they do not know and/or do not trust. Users should either delete the email in question or notify the support staff for further investigation.

Virus protection and prevention software will be activated on all computing devices. All remote-access information systems, to include PDA's (where applicable and feasible) and wireless email devices (Blackberry, etc.), will be programmed to perform periodic virus checks while the device is turned on.

Each agency will implement virus-reporting procedures to support Computer Incident Response Team (CIRT) reporting requirements. Immediate notification to the CIRT should occur if any desktop system alerts of virus notification to the user. Once a device is infected with a virus, the offending machine should be removed from the network until such time the virus can be removed from the machine. If ISD detects that a machine located on an Agency local network is infected with a virus, access will be blocked from the rest of the State network to/from that machine so the virus will not be spread to other machines on the State network. When the Agency notifies ISD that the virus has been removed, access will be restored.

ISD will use a multi-level approach to virus prevention and detection by deploying one virus-scanning engine on the workstations/personal computers and a different virus-scanning engine on servers.

ISD shall install real-time anti-virus (AV) software on all file servers to limit the spread of viruses on the network. Scanning of files will occur continuously to ensure viruses are detected quickly and responded to appropriately. All new files, including new “shrink-wrapped” COTS software, will be scanned with an AV product before introduction onto State networks.

ISD will notify users of new viruses and ensure virus patterns are updated at a minimum weekly, or as directed by the CIRT for immediate threat reduction. Virus definition availability is based on vendors’ capabilities, and personnel shall institute processes to automatically update definitions as published or available from authorized ISD Web sites.

ISD shall review anti-virus activity logs weekly to ensure the anti-virus software is functioning properly.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Spyware: software that sends information about your Internet sessions back to the computer from which it's launched, often used to create marketing profiles based on surfing habits, it's typically built into free Internet downloads and works in the background without the user's knowledge or permission.

Virus: a code fragment (not an independent program) that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources, which are then not available to authorized users.

Worm: an independent program that reproduces by copying itself from one system to another, usually over a network. Like a virus, a worm may damage data directly, or it may degrade system performance by consuming system resources and even shutting down a network.

Trojan Horse: an independent program that appears to perform a useful function but that hides another unauthorized program inside it. When an authorized user performs the apparent function, the Trojan horse performs the unauthorized function as well (often usurping the privileges of the user).

Additional Information

Refer to ISD Information Security Policy 600-SA19, Computer Incident Response.

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Software Licensing		
Policy Number: 600-SA03	Version: DRAFT	Effective Date:

Purpose

The purpose of this policy is to prevent software piracy and ensure State of Alabama compliance with software license agreements. Software piracy is a Federal offense. Violations can result in both civil suit and criminal charges, fines of up to \$250,000.00 per title infringed, and possible imprisonment.

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information systems.

Policy

Software piracy is illegal and is absolutely prohibited.

ISD shall establish software approval and implementation procedures that include system integration testing, software vulnerability assessment, and virus scanning prior to installation on the State network.

Software installed on any State-managed computing or network device shall be documented and tracked by ISD to ensure the State of Alabama complies with all rules and requirements established by the vendor and defined in the software license agreement.

Software (including operating systems, utilities, services, and productivity tools) installed on every State-managed personal computer, workstation, or server shall comply with software configuration standards established by ISD and comply with all license agreements.

Acquisition of software for installation on State-managed computing equipment shall be reviewed and approved by ISD. Only ISD-approved software may be installed on State-managed computer systems. Freeware and shareware shall not be downloaded from the Internet or otherwise installed unless approved by ISD.

Software licenses for approved computer applications and operating systems are the property of the State of Alabama. ISD will routinely perform software audits to insure policy compliance.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Additional Information

See ISD Information Security Policy 600-SU09, Software Use.

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



STATE OF ALABAMA GOVERNMENT INFORMATION

Department of Finance Information Services Division

INFORMATION SECURITY POLICY

External Connections		
Policy Number: 600-SA04	Version: DRAFT	Effective Date: [Date]

Purpose

This document describes the conditions under which third party organizations connect to State of Alabama networks for the purpose of transacting State business. The purpose of this policy is to ensure that connections to systems external to State network systems are properly secured and sensitive information is safeguarded.

Scope

Any external system hosted on the State of Alabama network is subject to the standards and procedures written and used to implement this policy. Connections between third parties that require access to non-public State of Alabama resources also fall under this policy, regardless of whether a telephone company circuit (such as frame relay or ISDN) or VPN technology is used for the connection. Connectivity to third parties, such as the Internet Service Providers (ISPs) that provide Internet access for the State of Alabama or to the Public Switched Telephone Network, does NOT fall under this policy.

Policy

All connections to external networks must be approved by and managed by the Information Services Division (ISD) of the Department of Finance. Connections will be allowed only with external networks that have been determined to have acceptable security controls and procedures.

Establishing Connectivity: Sponsoring Organizations within the State of Alabama that wish to establish connectivity to a third party are to file a new site request with the ISD network group. The Sponsoring Organization must provide the network group a valid business justification for the proposed access. The network group will engage the Security Council to address security issues inherent in the project.

The ISD Security Council shall review all new external connection requests. Reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least privilege is followed. This review may entail detailed vulnerability assessment by an independent third party at the expense of the State or the requesting organization to further assess the risk to State assets due to the external connectivity.

New external connections shall be treated as engineering changes to the State network and shall follow the engineering change proposal process defined in the ISD Security Council Procedures to ensure the security and configuration control of the State network baseline.

Network connection with external networks, and users outside the organization's domain, shall be protected by a network firewall and a DMZ.

Appropriate filtering, authentication, logging, and restrictions shall be instituted to ensure the proprietary network is secured. In no case will the State of Alabama rely upon the third party to protect the State of Alabama's network or resources. Third Party firewalls shall be subject to review and policy assessment to ensure the State network is receiving appropriate protection.

Third Party Connection Agreement: All new connection requests between third parties and State of Alabama require that the third party and State of Alabama representatives agree to and sign the Third Party Agreement. This agreement must be signed by an executive of the Sponsoring Organization as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the network group.

Point of Contact: The Sponsoring Organization must designate a person to be the Point of Contact (POC) for the external connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this policy and the Third Party Agreement that pertain to it. In the event that the POC changes, the network group or designated Project Manager must be informed promptly.

Use of Extranet connections must not reduce the confidentiality, integrity or availability of critical and essential applications and/or the State network. Accordingly, any extranet connections into and/or across the State must comply with the security standards described below for authentication and authorization. Additionally, the monitoring, reporting and user awareness requirements as set forth in ISD Information Security Policy 600-SA05, Extranet Management, shall be complied with.

Authentication. Access to the Extranet will be limited to authorized users and authenticated partner networks and network devices. Authentication will be performed using an encrypted message format to ensure confidentiality of authenticating information. VPN user accounts are not to be shared. There will be no clear-text or unauthenticated access to the Extranet. See the State of Alabama VPN policy for more guidance.

Authorization. Authorization to the Extranet will be granted by ISD to the requesting organization upon request from that organization director or other responsible party. At a minimum, the request should include:

- Requesting organization
- Personnel requiring access
- Hours required for access
- Business case

- Duration / Expiration of access requirement

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Circuit: For the purposes of this policy, circuit refers to the method of network access, whether it's through traditional ISDN, Frame Relay etc., or via VPN/Encryption technologies.

Extranet. The extension of a agency's intranet out onto the Internet to allow selected customers, suppliers and mobile workers to access the company's private data and applications via the World Wide Web. This is in contrast to, and usually in addition to, the agency's public web site (which is accessible to everyone). Generally an extranet implies real-time access through a firewall. Such facilities require very careful attention to security.

Least Privilege: This principle requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Sponsoring Organization: The State agency requesting that the third party be granted access into State network.

Third Party: A business that is not a formal or subsidiary part of the State.

Additional Information

Related policy: ISD Information Security Policy 600-SA05, Extranet Management

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release

ALABAMA

STATE OF ALABAMA GOVERNMENT INFORMATION

Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Extranet Management		
Policy Number: 600-SA05	Version: DRAFT	Effective Date: [Date]

Purpose

Policies for extranet systems management are essential to safeguard security of Statewide-connected network systems, and ensure that a baseline level of connection service quality is provided to a diverse user community. This policy sets forth the requirements for management of the State of Alabama extranet and assigns responsibilities for the deployment of extranet services by all State agencies. It refines and extends the State External Connections policy and other relevant policies by adding specific content addressing extranet management. Policy statements in this document generally provide for the Information Systems Division (ISD) of the Department of Finance to support the publicly accessible extranet environment that is in place now and future expansion of the extranet environment.

Scope

This ISD Information Security Policy applies to all administrators and managers (whether State of Alabama employees, contractors, vendors, or business partners) of any State-managed information systems supporting extranet services

Policy

Extranet services shall be managed by ISD for all State agencies.

Extranet clients accessing the infrastructure must meet certain standards to ensure only authorized and authenticated users connect to the campus network and that organizational data used by State users and systems not be exposed to unauthorized individuals.

Privilege Access Controls: All computers permanently or intermittently connected to either external networks or State networks must operate with privilege access controls approved by ISD. Multi-user systems must employ user IDs unique to each user, as well as user privilege restriction mechanisms including directory and file access permissions. Network-connected single-user systems must employ approved hardware or software mechanisms that control system booting and that include a time-out-after-no-activity screen blanker.

Anti-Virus and Firewall Protection: External computers or networks making remote connections to State internal computers or networks must utilize an up-to-date, active virus scanning and repair program, and an active personal firewall system (hardware or software).

Time-Out: All systems accepting remote connections from public network connected users (users connected through dial-up phone modems, Internet Service Providers, cable modems, etc.) must apply a time-out feature. This time-out feature must terminate all sessions after no more than 30 minutes of inactivity. An absolute time-out will occur after 24 hours of continuous connection and will require reconnection and authentication to re-enter the network. In addition, all user-IDs registered to networks or computers with external access facilities may be automatically suspended after a period of 30 days of inactivity.

All systems accepting remote connections from public network connected users (users connected through dial-up phone modems, Internet Service Providers, cable modems, etc.) must temporarily terminate the connection or time-out the user ID following a series of three unsuccessful attempts to log-in.

Extranet use shall be monitored on a regular basis for security and performance.

Authentication, authorization, usage and extranet performance reports shall be published monthly. Reports shall include, but not be limited to, the following:

- Successful and failed authentication attempts
- Extranet downtime due to network degradation
- Extranet Performance metrics
- Extranet usage metrics

Reports shall be maintained in accordance with State data retention requirements.

With the exception of web servers, electronic bulletin boards, or other systems where all regular users are anonymous, users are prohibited from remotely logging into any State system or network anonymously (for example, by using “guest” user IDs). If users employ systems facilities which allow them to change the active user ID to gain certain privileges, they must have initially logged-in employing a user ID that clearly indicates their identity.

All changes in access must be accompanied by a valid business justification, and are subject to security review. The Sponsoring Organization is responsible for notifying the network group when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

When access is no longer required, the Sponsoring Organization must notify the network group responsible for that connectivity, which will then terminate the access.

The network group must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still necessary and justified, and that the access provided meets the needs of the connection. Connections that are depreciated, or no longer being used to conduct State business, will be terminated immediately.

The internal addresses, configurations, and related system design information of State computers and networks is confidential and must not be released to third parties who do not have a demonstrable need-to-know such information. Likewise, the security measures employed to protect State computers and networks are confidential and shall be similarly protected.

A security incident or a depreciated circuit that is no longer being used to conduct State business necessitates a modification of existing permissions, or termination of connectivity. The network group will notify the POC of the Sponsoring Organization of the change prior to taking any action.

Any unusual extranet event indicating possible unauthorized use of extranet services shall be immediately reported as a computer security incident following applicable procedures. The Computer Incident Response Team (CIRT) will take appropriate action.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Extranet: The extension of a agency's intranet out onto the Internet to allow selected customers, suppliers and mobile workers to access the company's private data and applications via the World Wide Web. This is in contrast to, and usually in addition to, the agency's public web site (which is accessible to everyone). Generally an extranet implies real-time access through a firewall. Such facilities require very careful attention to security.

Sponsoring Organization: The State agency requesting that a third party be granted access into State network.

Third Party: A business that is not a formal or subsidiary part of the State.

Additional Information

Related policy: ISD Information Security Policy 600-SA04, External Connections

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release

ALABAMA

STATE OF ALABAMA GOVERNMENT INFORMATION

Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Asset Protection		
Policy Number: 600-SA08	Version: DRAFT	Effective Date: [Date]

Purpose

This policy continues the discussion of the physical security of computing equipment and data that must be practiced by all computer users to ensure the safeguard of State of Alabama computing and intellectual property. Implementation of the policies contained herein will primarily be the responsibility of designated System Administrators.

Scope

This Information Services Division (ISD) Information Security Policy applies to all administrators of any State-managed information systems (whether State of Alabama employees, contractors, vendors, or business partners) and their management.

Policy

Servers, switches, routers, hubs, and telecommunication switches shall be located in secured and environmentally controlled areas. Physical access shall be controlled by the use of key locks (with limited distribution), access code keypads, or access control cards. A record shall be maintained of personnel who have been granted the access method whether by key, code, or card. Access codes shall be changed periodically.

Access to servers and communications equipment shall be limited to authorized technical service personnel. Maintain a list of all personnel authorized to access servers and communications facilities. ISD management, or a designated user manager, shall approve authorization for access to facilities and equipment.

Visitors must present Government-issued photo identification, and the information must be recorded to a visitor access log, prior to the visitor being granted access to controlled areas or areas containing sensitive data (e.g., data storage facilities). The receptionist, guard, escort, or person granting access should complete the visitor log, not the visitor. Visitors must be escorted or in the company of a State employee at all times.

Equipment should be stored in racks where feasible and in all cases shall be stored above the floor, or on a raised floor, to prevent damage from dampness or flooding.

Each facility containing computer and communications equipment shall have a class C fire extinguisher (readily available and in working order) or an appropriate fire suppression system.

Electronic media shall be stored in fire safe containers in an environmentally controlled area.

Backup/archive media shall be stored in a secure off-site storage facility.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Additional Information

Additional policies on physical security pertaining to all users are found in ISD Information Security Policy 600-SU03, Physical Security.

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Applications Security		
Policy Number: 600-SA11	Version: DRAFT	Effective Date:

Purpose

The State network provides for very definitive control and management of user access to network and server resources. In addition to the network security many applications also provide security features and options that ensure the protection of the information and data within that specific application. With over 70% of successful Internet attacks now exploiting application vulnerabilities, this layer of application security is a critical element in protecting the State's confidential and sensitive data and controlling access to that data. This policy expresses the requirement to ensure application security for State of Alabama production applications.

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information systems, and to all applications hosted on the State network, intranet or extranet.

Policy

State of Alabama production applications shall provide a level of security and access controls appropriate to the confidentiality and risk inherent in the data being processed. This shall be based on a thorough application Information Security Risk Assessment.

Applications shall in no way disable, change, or circumvent any security controls in place in the network or other applications.

Prior to placing any new application on the State network an initial risk assessment shall be completed to evaluate and document system and application level controls.

Establish procedures and supporting processes to routinely assess existing applications against current industry standards and emerging threats.

New applications being developed shall have security designed in from the start.

Ensure developers are properly trained and equipped to build and deliver secure applications. Developers should be given guidelines for developing secure code as well as tools to help them check applications for possible security flaws.

Application users shall be granted application access and authorization commensurate with their informational needs and their job roles and responsibilities. A formal record of all authorized application users shall be maintained by the application owner and shall be current at all times. Changes to the current level of user access shall be documented and approved by the user's supervisor, the application owner, or designated security administrator.

Administrator rights shall only be granted to Application System Administrators or designated applications security administrators. The assignment of application administrator rights shall be limited and all assignment of application administrator rights and privileges shall be documented and approved by the system owner.

Access to applications shall be governed by an appropriate set of application user profiles that outline the level of access granted and the functions permitted. User profiles shall be developed, documented, and approved by the system owner for each production application. These profiles define the rights and privileges assigned to the user based on their job function and their level of authority within the business application.

Enforce Least Privilege. The concept of least privilege is universally accepted as a basis for security systems. Accounts shall not have access to more information than is required for the account owner to do their job.

Application owners shall ensure the activities on their application(s) are appropriately monitored and logged. Monitoring and logging shall provide an audit trail that can identify the user, the time and date, and the actions performed based by the user (see ISD Information Security Policy 600-SA17 Audit Policy for additional audit requirements).

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Least Privilege: This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Additional Information

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Remote Access		
Policy Number: 600-SA13	Version: DRAFT	Effective Date:

Purpose

The increasing mobility of State employees and contractors has made remote access to State network resources vital to conducting State business. This policy sets forth the responsibilities for using and administering remote access capabilities for access to State network resources. It refines and expands the State Network Access Policy (Information Security Policy 600-SU04) and other relevant policies by adding specific content addressing remote access communications. The policy is meant to ensure remote access technologies are deployed to ensure State systems maintain acceptable levels of security and service.

Scope

This Information Services Division (ISD) Information Security Policy applies to all State of Alabama employees, contractors, vendors, or business partners who remotely access (via dial-in modem, cable modem, frame relay, ISDN, DSL, etc) any State-managed information systems and to all personnel responsible for the administration of remote access services.

Policy

Remote access users must understand the State is providing the same basic access to the network that a user would see from a network-connected work location. Users shall comply with all applicable laws and policies regarding access to their network account. Furthermore, the State expects that users will be security-minded when using remote access.

ISD, the State's primary provider and administrator of remote access network services, will provide their best effort to make remote access available at all times. Because some factors are beyond control, ISD makes no guarantee of accessibility to its remote access servers, especially during peak usage periods.

User Responsibilities

It is the responsibility of State employees, contractors, vendors and agents with remote access privileges to the State network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the State.

The State is not responsible for communications service charges the user incurs as a part of connecting to the State network. The user shall bear any cost imposed by the communication service provider (telephone company, ISP, etc) when the user connects to the State network using a remote access method.

State employees and contractors with remote access privileges must ensure that their State-owned or personal computer or workstation, which is remotely connected to the State network, is not connected to any other network at the same time (with the exception of personal networks that are under the complete control of the user).

Personal equipment used for remote access connection to State networks must meet the requirements of State-owned equipment.

All hosts, including privately owned personal computers, connected to State networks via remote access must have the most up-to-date anti-virus software and current operating system service pack and patch level.

Users with remote access privileges to the State network must not use non-State email accounts (e.g., Hotmail, Yahoo, AOL) or other external resources to conduct State business.

Administrator Responsibilities

Do not divulge details or instructions regarding remote access, including external network access points or dial-up numbers, unless the requester has been verified as authorized to connect to the State network as an external user.

Routers for dedicated ISDN lines configured for access to the State network must meet minimum authentication requirements of CHAP.

Frame Relay must meet minimum authentication requirements of DLCI standards.

Dual-homing is not permitted.

Secure remote access shall be strictly controlled. Where possible, control will be enforced via one-time password authentication or public/private keys with strong pass-phrases.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

CHAP: Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function.

DLCI: Data Link Connection Identifier is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dual Homing: Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the State network via a local Ethernet connection, and dialing into AOL or other Internet Service Provider (ISP). Being on a State-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into State and an ISP, depending on packet destination.

Frame Relay: A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

ISDN: There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels-at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access: Any access to the State network through a non-State controlled network, device, or medium.

Additional Information

All remote access users and administrators should be familiar with and comply with all ISD Secure User policies. Additionally, administrators and users should refer to the following policies extending the requirements of remote access as pertains to virtual private networks (VPNs) and wireless devices:

ISD Information Security Policy 600-SA14, VPN Communications

ISD Information Security Policy 600-SA15, Wireless/Mobile Devices

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

VPN Communications		
Policy Number: 600-SA14	Version: DRAFT	Effective Date:

Purpose

The purpose of this policy is to provide requirements for remote access IPSec Virtual Private Network (VPN) connections into the State of Alabama network.

Scope

This Information Services Division (ISD) Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) authorized to use a VPN to access the State network (users) and to all personnel responsible for the administration of VPN services and devices (administrators).

Policy

Approved State employees and authorized third parties (consultants, vendors, etc.) may utilize State VPN capability. Access (VPN and otherwise) to the State internal network from remote locations including homes, hotel rooms, wireless devices and off-site offices is not automatically granted to users in conjunction with network or system access. Systems that contain confidential personnel and financial data will be available for off-site remote access only after an explicit request is made and approved by the data steward for the target system. Access will be permitted through a centrally managed VPN that provides encryption and secure authentication. Access may be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor, or negative impact on overall network performance attributable to remote connections. Remote access privileges will be reviewed upon an employee's change of departments.

User Responsibilities

When using VPN technology with privately owned personal computers, users must understand that their systems are a de facto extension of the State of Alabama network, and as such are subject to the same rules and regulations that apply to State-owned equipment, i.e., their systems must be configured to comply with ISD Security Policies and standards.

All hosts, including privately owned personal computers, connected to State networks via VPN (or any other remote access technology) must have the most up-to-date anti-virus software and current operating system service pack and patch level. All hosts may be scanned to ensure compliance with this policy, and users may be denied VPN access if their host system presents an unacceptable risk to State networks.

The VPN user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

VPN users will be automatically disconnected from the State network after a prescribed period of inactivity (see applicable Standard). The user must logon again to reconnect to the network. Pings or other artificial network processes shall not be used to keep the connection open.

Dual (split) tunneling is not permitted; only one network connection is allowed.

Administrator Responsibilities

ISD, the State's primary provider and administrator of VPN services, will administer VPN access points.

No VPN shall provide access to the state network infrastructure without first requiring user-level authentication and creating an encrypted session.

- VPNs shall enforce user authentication at the access point before granting access to state network or Internet services.
- VPNs shall use 168-bit 3DES encryption (or stronger).

When actively connected to the State network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.

On a recurring basis, ISD shall accomplish validation of existing VPN connections and authorized users. This validation process allows ISD to determine whether the VPN is still required for the agency or individual in question.

VPN usage shall be monitored on a regular basis for security and performance. Any unusual VPN event that may reflect unauthorized use of VPN services shall immediately be reported as a computer security incident following applicable procedures.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

3DES: Triple Data Encryption Standard, or “Triple DES”, a mode of the DES encryption algorithm that encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with the second key, and the resulting cipher text is again encrypted with a third key).

IPSec: Internet Protocol Security; a set of protocols that support secure exchange of packets at the IP layer; supports implementation of Virtual Private Networks (VPNs).

Split-tunneling: Simultaneous direct access to a non-State network (such as the Internet, or a home network) from a remote device (PC, PDA, etc.) while connected into the State network via a VPN tunnel.

Tunnel: The encrypted session between two endpoints. To the user at the remote end, it appears as if connected to the internal LAN. This connection rides over the public Internet, hence the “tunnel.”

Virtual Private Network (VPN): A method for accessing a remote network via "tunneling" through the Internet.

Additional Information

Refer to ISD Information Security Policy 600-SA13, Remote Access

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance
Information Services Division

INFORMATION SECURITY POLICY

Wireless Networking		
Policy Number: 600-SA15	Version: DRAFT	Effective Date:

Purpose

This policy describes how wireless technologies are to be deployed, administered and supported by State of Alabama entities, whether controlled by the Information Services Division (ISD) of the Department of Finance or another State agency. It refines and expands the mobile device usage policy and other relevant policies by adding specific content addressing wireless network-level devices (access points, routers, bridges, VPN appliances, and management gateways). This policy couples the desire for State agencies to deploy wireless technologies with a central administrative desire to assure that all constituents be assured of deploying such systems with an acceptable level of service quality and security.

Scope

This ISD Information Security Policy applies to all administrators and managers (State of Alabama employees, contractors, vendors, and business partners) of any State-managed wireless networking systems.

Policy

Use layer 2 or 3 encryption with Advance Encryption Standard (AES). Layer 3 encryption, with a FIPS 140-2 secure VPN solution, is used to secure WLAN traffic to the internal network. This approach has the advantage of treating wireless access the same as remote access from the Internet for organizations already equipped with VPN capability.

Client devices connecting remotely shall meet the requirements for mobile devices as stated in ISD Information Security Policy 600-SU10, Mobile Devices. Ensure only approved devices, applications, and network/PC connection methods and wireless services are used for mobile computing.

The wireless network administrator (hereafter simply ‘administrator’) shall maintain a list of all wireless devices by type, model number, serial number, and location. For WLAN devices, the list shall include MAC address and user information.

The administrator shall ensure that WLAN systems are compliant with overall network security architecture.

The administrator shall ensure that wireless devices, which connect directly or indirectly (hotsync) to the network, are added to site network diagrams.

Disable management ports on network devices when not in use. In addition to physical access controls, secure and strongly authenticated network access is required in order to manage the Access Point (AP) in any highly sensitive environment. Secondary protection if this capability is not available would be to password protect the port with strong two factor authentication.

Do not manage APs from wireless interfaces. Instead, manage the devices from a separate, wired VLAN that is used only by network administrators with proper authentication credentials using appropriate tools (e.g., Secure Shell (SSH)).

Enable Wireless Client Isolation. Disallow wireless clients from communicating with each other through an access point unless there is a business requirement for such communication.

The administrator shall ensure that vendor supported, State approved, anti-virus software is installed on all wireless, handheld, or mobile devices and configured in accordance with applicable policies and kept up-to-date with the most recent virus definition tables.

Administrators shall ensure that SSIDs are changed from the manufacturer’s default to a pseudo random word consisting of a combination of characters, numbers, and special characters. If possible, the new SSID should follow network password rules. Choose an SSID that does not readily identify the agency or State.

SSID broadcast mode shall be disabled. Disabling SSID broadcast mode requires users to know the network name before associating. This setting does not prevent an experienced attacker from discovering the network’s SSID but should be viewed as a part of a multilayered security posture. WLAN APs that do not allow the SSID broadcast mode to be disabled shall not be used.

Ensure APs and bridges are password-protected. Change passwords from the manufacturer's default setting. Use strong passwords consistent with OIT Information Security Policy 600-SU08, Passwords.

MAC address filtering shall be enabled at each AP. Enable MAC address filtering from a central server if automatic device network registration is operational within the enterprise. If automatic network registration is not operational, manual registration for an enterprise is probably not justified for wireless devices. This setting does not prevent an experienced attacker from discovering and spoofing an authorized MAC address but should be viewed as a part of a multilayered security posture.

Association with APs outside the firewall shall not be allowed.

APs shall be placed in a screened subnet (DMZ), or Virtual LAN (VLAN) and separated from the wired internal network. A VPN shall be placed between the AP and the LAN.

The administrator shall ensure WLAN APs are set to the lowest possible transmit power setting that meets the required signal strength of the area serviced. This is a precaution that can be easily thwarted by an attacker with a powerful antenna. Set AP transmit power to appropriately balance needs for coverage, interference, and security.

If the WLAN provides seamless roaming between APs (session persistence), the WLAN shall provide session timeout capability. The session timeout shall be set for 30 minutes or less. This feature mitigates the risk of an abandoned, authenticated session being hijacked by an unauthorized attacker.

Ensure AAA services are used for identification and authentication of the user on WLAN systems.

A firewall shall be used to block Address Resolution Protocol (ARP) cache poison attacks and provide an additional layer of protection for the wired network.

Ensure an Intrusion Detection System (IDS) is used to monitor the wireless network.

Ensure enterprise level network products select can save backup configuration files onto another device (backup area on server). This requirement is similar to saving wired router configurations in compliance with best practices for disaster recovery preparedness.

Enable and configure logging. Review logs frequently.

The administrator shall ensure that procedures for hot-syncing sensitive information to the PDA include the following:

- Hot-sync management software shall only be launched when hot-syncing the PDA and closed as soon as the hot-sync operation has completed.
- Hot-sync management software shall not be launched as part of the computer boot-up process, if the software does not require a password before use.

- Synchronization access control software is installed on all workstations that have synchronization software installed on them, if available.
- PDAs that transfer, receive, store, or process sensitive information shall not be synced to home or personally owned PCs.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

SSID: Service Set Identifier, a network name that differentiates one WLAN from another.

Additional Information

ISD Information Security Policy 600-SU10, Mobile Devices

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release



Department of Finance Information Services Division

INFORMATION SECURITY POLICY

Computer Incident Response		
Policy Number: 600-SA19	Version: DRAFT	Effective Date:

Purpose

The purpose of this policy is to ensure the Information Services Division (ISD) of the Department of Finance is prepared to respond to computer incidents. A computer incident is defined as a security event that produces actual or potentially adverse impact on computer and network operations (see Definitions below). Computer incidents may include:

- Unauthorized access to a system and/or to the data in the system
- Denial of Service (DoS) attack or other disruptions to service
- System changes that are not authorized nor known to the system owner
- Repeated attempts to gain unauthorized access to systems and/or data

Scope

This ISD Information Security Policy applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information systems.

Policy

All users of State of Alabama computing resources shall be aware of what constitutes a computer incident and shall understand incident reporting procedures.

Computer Incident Response Procedures shall be developed to ensure management and key personnel are notified of computer incidents as required. Procedures shall designate a single point of contact for reporting all computer incidents.

A Computer Incident Response Team (CIRT) shall be established and supported to ensure appropriate response to computer incidents. This team shall consist of members of ISD and key personnel from other agencies. CIRT responsibilities shall be defined in the Computer Incident Response Procedures.

The CIRT shall manage ongoing communications aspects of an incident, including press release and notification of law enforcement if warranted.

All computer incidents shall be documented. Documented information shall include system logs, audit logs, security alert messages, records of the violation, and copies of affected data or

information. Retain and safeguard computer incident documentation as evidence for investigation, potential disciplinary actions, and/or prosecution.

Enforcement

Refer to ISD Information Security Policy 600-SU01, Commitment to Information Security.

Definitions

Computer Incident: Security events that have a real impact on the organization (when damage is done, access is achieved by the intruder, loss occurs, or malicious code is implanted), or when detecting something noteworthy or unusual (new traffic pattern, new type of malicious code, or a specific IP as a source of persistent attacks) having the potential to impact the organization.

Denial of Service (DoS) Attack: Multiple service requests sent to a victim's computer until it eventually overwhelms the system causing it to freeze, reboot, and ultimately not be able to carry our regular tasks (examples are SYN Flood, Ping of Death, etc).

Security Event: routine probes, ping sweeps, port scans, etc.

Additional Information

Computer Incident Response Procedures (not yet published)

Revision History

Version:	Release Date:	Comments:
1.0	Pending	Initial Release