

STATE OF ALABAMA

Information Technology Policy

POLICY 630-01: SYSTEM USE

Inappropriate use of State information technology (IT) resources exposes the State and its data to risks including potential virus attacks, compromise of network systems and services, and legal liabilities. 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 IT user to know these rules and to conduct their activities accordingly. These rules are in place to protect the employee, the State, and the State's data.

OBJECTIVE:

Define acceptable and non-acceptable use of State-owned IT resources including systems and devices, software, Internet, and communications capabilities including e-mail, instant messaging, and social media.

SCOPE:

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

SYSTEM USE POLICIES

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, and 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 the people it serves in the course of normal operations.

PERSONAL USE:

Limited personal use of State-managed computing resources is anticipated; however, employees and managers are responsible for exercising good judgment regarding the reasonableness of personal use.

Agencies may create additional policies concerning personal use of State information systems, but no agency policy may impose a lesser limitation on personal use than is prescribed by this policy.

PROHIBITED ACTIVITIES:

The following activities are prohibited when using State IT resources:

- Any activity that is illegal under local, state, federal or international law
- Non-incident personal use of State-managed computing resources
- Activities in support of personal or private business enterprises
- Unauthorized reproduction of copyrighted material
- Violating the rights of any person or other legal entity protected by copyright, trade secret, patent or other intellectual property laws, or similar laws or regulations, including, but not limited to, laws which protect against the installation or distribution of software products that are not appropriately licensed for use by the State
- Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws

- Introducing malicious software (malware) into the network or systems (e.g., viruses, worms, Trojan horses, logic bombs, etc.) within reason of user's control
- Making fraudulent offers of products or services
- Making statements of warranty, expressed or implied, unless part of normal duties
- Accessing, possessing, or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction
- Accessing, possessing, or transmitting any sexually explicit, offensive, or inappropriate images and/or text
- 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 within the scope of regular duties; potential disruptions include, but are not limited to, port/IP scanning, packet sniffing, or IP spoofing)
- Conducting network, system, or application scanning without IT Manager prior approval
- 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
- Accessing web sites offering online gambling, 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

EXCEPTIONS:

Employees may be exempted from some of these restrictions in the course of their legitimate job responsibilities (e.g., Investigative personnel may require access to web sites that are otherwise restricted).

IT Managers or Agency Heads shall request exceptions from the appropriate authority (e.g., Network Support, State IT Security Council, or CIO).

INTERNET ACCESS POLICIES

Access to the Internet is provided as a business and informational resource to support and enhance the capability of Internet users to carry out their job responsibilities. Internet users are expected to handle their access privileges in a responsible manner and to follow all Internet-related policies and procedures.

The State reserves the right to access, monitor, or disclose all Internet activity as required in the course of monitoring, auditing, or responding to legal processes or investigative procedures.

Users do not enjoy any right of personal privacy when using State-provided Internet services. All records created as a result of using Internet services are government records. As such, these records are subject to the provisions of state laws regarding their maintenance, access, and disposition.

Internet usage records may be public records under the Alabama public records laws and may be made available to the public upon lawful request. If an agency deems their use of Internet services is an exception to the public records laws, the Agency Head shall request exception through the State Records Commission.

It is the responsibility of the Agency Head or Agency IT Manager to:

Ensure that each employee, agent, contractor, or other person utilizing Internet services has been advised of and understands all policies and restrictions applicable to the use of such services.

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.

INTERNET CONTENT MANAGEMENT:

Use of Internet resources for the purpose of accessing online games, Internet gambling sites, and viewing or downloading content inappropriate for official State business exposes the State and its data to risks including virus attacks, spyware and other malware threats, compromise of network systems and services, and potential legal issues. To mitigate these risks, access to certain categories of Internet content is restricted (blocked).

By the authority of the State CIO, the following categories of Internet content present a threat to the security of State systems or have been deemed not necessary for conducting official State business and are therefore blocked:

- Pornography/Nudity
- Gambling
- Online Games
- Spyware/Malware Sources and Effects

Exceptions may be granted to access blocked web sites for individuals or agencies that have a business need for access in order to do their jobs. Each request for access to a blocked web site requires a legitimate business need and written approval of the agency head or IT Manager and the State CIO.

E-MAIL USAGE POLICIES

To ensure the integrity and availability of e-mail system resources all electronic communications are expected to comply with relevant Federal and State laws as well as State policies and standards. The following requirements apply to the use of State-provided e-mail systems.

E-mail shall be distributed, stored, and disposed of based on the data content in accordance with State information management requirements.

E-mail content created, stored, transmitted, or received using State resources are the property of the State. Nothing in this policy shall be construed to waive any claim of privilege or confidentiality of e-mail content. Authorized State personnel may access, monitor, or disclose e-mail content for state business purposes or to satisfy legal obligations.

PERSONAL USE OF STATE E-MAIL:

State e-mail systems are to be used for business purposes in serving the interests of the government and of the people it serves; however, incidental, occasional personal use of State e-mail is permitted.

Employees and managers are responsible for exercising good judgment regarding the reasonableness (frequency and duration) of personal use.

In accordance with The Code of Alabama, Section 36-25-5, state e-mail shall not be used for "personal gain."

Personal e-mail shall be deleted or saved separately from work-related e-mail.

Users are permitted to include personal appointments in their Outlook calendar to help eliminate scheduling conflicts.

Users may store personal contact information in their Outlook contacts folder.

PROHIBITED USES OF STATE E-MAIL:

State e-mail systems shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive (vulgar or pornographic) content or offensive comments about a person's race, gender, age, appearance, disabilities, political beliefs, or religious beliefs and practices. Employees who receive any e-mail with this content from any State employee should report the matter to their supervisor immediately. Additional prohibited uses of e-mail are addressed in State standards.

In addition, the following activities are prohibited:

- Sending or forwarding remarks and/or images considered obscene, offensive, racist, libelous, slanderous, or defamatory (as defined, where applicable, in The Code of Alabama 1975)
- Using an individual State e-mail account to send or forward virus or malware warnings, security advisories, terrorist alerts, or other official warning, alert, or advisory messages without prior approval of the agency IT Manager, Agency Information Security Officer, or Chief Information Security Officer (unless in the course of normal assigned duties)
- Sending unsolicited e-mail messages including junk mail, spam, or other advertising material to individuals who did not specifically request such material except in the execution of normal government information dissemination
- Postings to newsgroups by personnel using a State e-mail address unless in the course of business duties
- Using State e-mail for personal or commercial ventures, religious or political causes, endorsement of candidates, or supporting non-government organizations
- Sending or forwarding chain letters or joke e-mail
- Disguising or attempting to disguise your identity when sending e-mail
- Sending e-mail messages using another person's e-mail account
- Intercepting e-mail messages destined for others
- Unauthorized use, forging, or attempting to forge e-mail header information or messages

AUTO-FORWARDING STATE E-MAIL:

To preclude inadvertent transmission of inappropriate information onto the Internet, auto-forwarding shall not be used to send State e-mail to an Internet e-mail address.

MASS E-MAIL:

Material sent to group distribution lists must be relevant to the group being mailed and shall pertain to State business and/or serve the interests of State employees or constituents.

Message Content/Format:

Message format may be text, HTML, or RTF and should not include attachments.

HTML or RTF format messages may contain artwork, but shall be limited to a single page.

Each message shall contain a signature block with the sender's name, departmental affiliation, office telephone number, and e-mail address.

Sender is responsible for all replies, responses, and complaints.

Message Approval:

It is the responsibility of the sender/requestor of a mass e-mail to obtain the necessary approval from the person, group, or designated owner of the distribution list.

Authority to use the "all-employees" distribution list rests with the Governor's office.

Approval authority for agency/organization-level groups (e.g., "ISD – All Users") shall rest with the manager or management team presiding over that group.

Message shall include a line indicating the State office that approved the mass e-mail.

Message Transmission:

Mass electronic mailings shall only be transmitted in the evenings (after 5pm).

List Owner Responsibilities:

Owners of group distribution lists shall develop and monitor compliance with written operating procedures for the use of their lists. All list owners are encouraged to consider the benefits of moderating or otherwise controlling access to large lists. This applies whether a list has been created for one-time use or is maintained as a standing list.

INSTANT MESSAGING POLICIES

Instant Messaging (IM) is subject to many of the same threats as e-mail (known security holes, information leaks, vulnerability to malware, etc.), and IM users are frequently the target of phishing attempts. For these reasons the following policies shall apply to all IM communications.

IM shall be used only for business communications (it is not provided for personal use).

IM shall not be used to communicate sensitive or confidential information.

IM shall be limited to text messages only; IM file transfers shall be blocked.

IM is correspondence that creates a record that can be subpoenaed and used as evidence in litigation or regulatory investigations; therefore, IM correspondence shall be retained in accordance with applicable State data and record retention policies.

IM content, created, stored, transmitted, or received using State resources, is the property of the State. Nothing in this policy shall be construed to waive any claim of privilege or confidentiality of IM content. Authorized State personnel may access, monitor, or disclose IM content for any business purpose or to satisfy legal obligations.

REMOVABLE STORAGE DEVICE POLICIES

Removable non-volatile storage devices (USB Flash drives, PC Cards, FireWire devices, MP3 players, camcorders, digital cameras, etc.) have the same vulnerabilities as disk media (malware, data loss) but greater capacity, and could be used to infect an information system to which they are attached with malicious code, could be used to transport sensitive data leading to potential compromise of the data, and are frequently lost or stolen. Careful attention to the security of such devices is necessary to protect the data they may contain. For these reasons the following requirements apply to the use of removable storage devices.

No removable storage device shall be attached to a State information system unless approved by the IT Manager.

The IT Manager shall maintain an inventory of all approved removable storage devices and ensure controls are in place to protect the confidentiality, integrity, and availability of State data.

Removable non-volatile storage devices shall be secured, marked, transported, and sanitized as required by State standards in the manner appropriate for the data category they contain.

Removable non-volatile storage devices shall, whenever possible, be formatted in a manner that allows the application of Access Controls to files or data stored on the device.

Sensitive or confidential data shall not be stored on any removable non-volatile storage device unless encrypted in accordance with applicable State standards. For devices that do not support encryption of the storage media, sensitive and confidential data shall, as promptly as possible, be transferred to a device that does support the required encryption and access controls. In the interim, the device

shall be securely stored apart from its storage media (whenever possible) and physical security must be assured. Organizational procedures shall clearly define the handling requirements for such data and devices, and device users shall be made aware of the risks and procedures.

Virus-scan all portable storage media (diskettes, CDs, USB drives, etc.) before files residing on the media are transferred or accessed.

Maintain physical security of removable storage devices. Report immediately the loss or theft of any device containing any State data.

User awareness training shall describe the risks and threats associated with the use of removable storage devices, the handling and labeling of these devices, and a discussion of the devices that contain persistent non-removable memory.

SOFTWARE LICENSING AND USE POLICIES

Under the provisions of U.S. copyright law, illegal reproduction of software can be subject to civil and criminal penalties including fines and imprisonment. Therefore, all system users must use only properly licensed software and must use that software in accordance with the terms and conditions of the license agreement.

Information Technology Users shall NOT:

- Copy, download, nor install unlicensed software
- Install personally-owned software onto State-managed computer systems
- Install State-owned software on any non-State-owned computer systems, including home computers, unless specifically authorized in the software license agreement

Agency IT Managers shall:

- Ensure only software that is licensed to the organization is installed and used
- Ensure software is installed and used in compliance with the license agreements
- Routinely perform software audits to ensure policy compliance
- Remove any software found on State information systems for which a valid license or proof of license cannot be determined

The term "software" includes the program, media, and licenses for all operating systems, utilities, services, and productivity tools whether freeware, shareware, open source, off-the-shelf, or custom-developed without regard to the system(s) on which it is installed (workstation, server, etc.).

SOCIAL MEDIA POLICIES

State agencies desiring to enhance their ability to communicate and interact with the public are turning to social media technologies such as weblogs, wikis, Facebook®, Twitter®, etc.

As with most technologies, social media poses certain risks including but not limited to:

- Adverse impact to network bandwidth
- Reputational risk to personnel, the agency, and the State
- Potential exposure or leakage of sensitive or protected information (such as copyrighted material, intellectual property, personally identifying information, etc)
- Potential avenue for malware introduction into the organization's IT environment

The following policies are established to address and minimize these risks and define the allowable and prohibited uses of social media technologies in the State IT environment.

SOCIAL MEDIA USE:

Organizations may utilize commercial social networking websites (such as Facebook and Twitter) or integrate social media capabilities (such as a wikis or weblogs) into State-hosted websites.

Information Services Division (ISD) Responsibilities:

ISD will provide security awareness training to educate users about the risks pertaining to social media and social networking, and provide best practices for risk remediation.

Agency Management Responsibilities:

- Conduct a formal assessment of the risk resulting from agency use of social media technologies.
- Assign appropriate personnel (Public Information Officer) to oversee the use of agency social media, evaluate and authorize agency requests for usage, and determine appropriateness of the content posted to social media sites.
- Understand that social media website contents are public records that must be retained and archived in accordance with applicable agency records disposition requirements.
- Obtain ISD approval before integrating social media capabilities on any websites hosted, developed, or administered by ISD.
- Periodically review social media usage to ensure it continues to reflect the agency's communication strategy and priorities.

Agency IT or Website Administrator Responsibilities:

- Disable (if possible) any unnecessary functionality within social media websites or applications, such as instant messaging (IM) and file upload/exchange.
- Minimize or eliminating links to other websites, such as "friends", to minimize the risk of exposing a government user to a link that leads to inappropriate or unauthorized material.
- Suppress any commercial or third-party advertisements (sometimes present when using freeware versions of social media software or tools).
- Monitor (and filter as necessary) all social media website content posted and/or viewed.
- Prohibit/block file uploads to the maximum extent possible. Where file uploads are allowed, ensure all user-submitted files are automatically virus scanned.
- Include appropriate statements on State-hosted social media sites advising users of the public nature of the information they post.

User Responsibilities:

- Social media may not be used for personal gain, conducting private commercial transactions, or engaging in private business activities.
- Understand that postings to social media websites immediately become part of a public record.
- Users shall not post or release proprietary, confidential, sensitive, personally identifiable information (PII), or other state government Intellectual Property on social media sites.
- Users who connect to social media websites through State information assets, who speak officially on behalf of the state agency or the State, or who may be perceived as speaking on behalf of an agency or the State, are subject to all agency and State requirements addressing prohibited or inappropriate behavior in the workplace, including acceptable use policies, user agreements, sexual harassment policies, etc.
- Users shall not speak in social media websites or other on-line forums on behalf of an agency, unless specifically authorized by the agency head or the agency's Public Information Office. Users may not speak on behalf of the State unless specifically authorized by the Governor.
- Users who are authorized to speak on behalf of the agency or State shall identify themselves by: 1) Full Name; 2) Title; 3) Agency; and 4) Contact Information, when posting or exchanging

information on social media forums, and shall address issues only within the scope of their specific authorization.

- Users who are not authorized to speak on behalf of the agency or State shall clarify that the information is being presented on their own behalf and that it does not represent the position of the State or an agency.
- Users shall not utilize tools or techniques to spoof, masquerade, or assume any identity or credentials except for legitimate law enforcement purpose or for other legitimate State purposes as defined in agency policy.
- Users shall use different passwords for different accounts; do not use the same password for both a social media site and state network or e-mail accounts.

Personal Use of Social Media Sites:

- Employees may use personal social media for limited family or personal communications during normal business hours so long as those communications do not interfere with their work. Employees and their managers are responsible for exercising good judgment regarding personal use.
- Users shall not use their state e-mail account or password in conjunction with a personal social media site.

Additional Recommended Security Measures:

For added security, all users of Facebook are encouraged to enable SSL activation in their Facebook account settings.

POLICY ENFORCEMENT

REPORTING:

Users should report security-related issues and policy non-compliance to their immediate supervisor, manager, or as outlined in the applicable information security policy, standard, or procedures.

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 through 13A-8-103), 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.

ADDITIONAL INFORMATION:

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
630-00	03/01/2011	This policy consolidates and replaces Policies 630-01 through 630-07 and Standards 630-01S1, 630-03S1, and 630-05S1.
630-01	09/01/2011	Added requirements for removable storage devices from Standard 680-01S3 (which is hereby rescinded).