

SAO
Appropriate Use and Monitoring
POLICY

Contents

PURPOSE.....	4
POLICY	4
NETWORK RESOURCES	5
INTERNET.....	5
EMAIL AND ELECTRONIC COMMUNICATIONS.....	5
REMOTE LOGIN.....	6
MOBILE DEVICES.....	6
USE OF STATE TELEPHONES.....	6
OTHER EQUIPMENT AND/OR SUPPLIES	7
INAPPROPRIATE USAGE.....	7
DOWNLOADS.....	7
HARDWARE INSTALLATION	8
PERSONAL USE OF AUDIO CDS, DVDS	8
PERSONAL USE OF ENCRYPTION	8
PROTECTION OF IT RESOURCES.....	8
PROPRIETARY INFORMATION.....	9
CONSENT TO MONITORING.....	9
ACCOUNTS AND ACCOUNT PASSWORDS	9
EXCEPTIONS.....	10
NON-COMPLIANCE	10

Version

Version	Date	Revision / Description	SAO Approval
1	11/13/2008	Original Document	Roger Smith
2	7/01/2013	Document Update	Roderick L Wright

STATE ACCOUNTING OFFICE
Security Policy
Appropriate Use and Monitoring Policy

EFFECTIVE DATE: *June 25, 2013*

RELEASE DATE: *July 1, 2013*

REFERENCE: *GTA Appropriate Use and Monitoring (SS-08-001)*
GTA Acquisition/Use of Telecommunication Services and Equipment (PM-04-002)
GTA Electronic Communications Accountability (SS-08-009)
GTA Email Use and Protection (SS-08-011)

PURPOSE

The State Accounting Office (SAO) Information Technology (IT) resources are provided to authorized users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations on Users and is subject to Georgia Technology Authority (GTA) policies and applicable State and Federal laws. It is the responsibility of Users to ensure that such resources are not misused.

SCOPE

The following Appropriate Use Policies applies to all SAO employees and Users of IT resources owned or managed by SAO. Individuals/ Users covered by the policy include (but are not limited to) SAO employees, contractors, vendors, external individuals and organizations accessing SAO IT resources.

IT resources for the purposes of this Policy include, but are not limited to, SAO-owned transmission lines, networks, wireless networks, servers, internet connections, terminals, applications, personal computers, and mobile devices. IT resources include those owned by the SAO and those used by SAO under license or contract, including but not limited to information recorded on all types of electronic media, computer hardware and software, paper, computer networks, and telephone systems.

POLICY

NETWORK RESOURCES

SAO employees, vendors/business partners, local governments, and other governmental agencies may be authorized to access State network resources to perform business function with or on behalf of the State. Users must be acting within the scope of their employment or contractual relationship with the State and must agree to abide by this policy. All usage may be monitored and there is no right to privacy. Various transactions resulting from network usage are the property of the State and are thus subject to open records laws.

INTERNET

SAO Employees are responsible for making sure they use this access correctly and wisely. Staff should not allow Internet use to interfere with their job duties.

Acceptable uses include:

- Access to and distribution of information that is in direct support of the business of SAO;
- Providing and simplifying communications with other State agencies, State of Georgia employees and citizens of Georgia;
- Communication of information related to professional development or to remain current on topics of general SAO interest;
- Announcement of new laws, rules, or regulations;
- Encouraging collaborative projects and sharing of resources.

Inappropriate uses of web access include, but are not limited to:

- Viewing, downloading or sending pornographic or other obscene materials;
- “Surfing” the Web for inordinate amounts of time;
- Otherwise endangering productivity of SAO;
- Purposes which violates a Federal or Georgia law;
- Dissemination or printing copyrighted materials (including articles and software) in violation of copyright laws.

EMAIL AND ELECTRONIC COMMUNICATIONS

Any information originating from a State electronic information system or State employee while acting in their official capacity could be interpreted as an official position of the State. As employees of the State we are custodians of the data we create, receive, transfer, and access. As such, we are individually responsible for

maintaining the image and integrity of the State by exercising due diligence and due care with regards to content and transmission of all electronic correspondence from the State information systems or its employees.

Each SAO staff member is given an e-mail account. It is the responsibility of the employee to use their account in accordance with State policy and in such a way that does not interfere with their duties.

Specifically prohibited in the use of e-mail is:

- Sending or forwarding any confidential data without encryption
- Any activity covered by inappropriate use Statements included in this policy;
- Sending, forwarding chain letters, virus, hoaxes, etc.;
- Sending, forwarding or opening executable files (.exe) or other attachments unrelated to specific work activities, as these frequently contain viruses;
- Use of abusive or profane language in messages;
- Submitting any large, unnecessary mail attachments;
- Use that reflects non-professional image of SAO.

REMOTE LOGIN

Access to SAO networks from remote locations shall be in accordance with the **SAO Remote Access Policy and Procedures**. Access is allowed through the use of SAO approved and provided remote access systems or software. SAO may allow remote access from non-State devices to access e-mail via a Web page.

MOBILE DEVICES

Employee's use of laptop computers or other electronic data mobile devices (e.g. Laptop, Blackberry, Flash Drive, Smart Phone, iPads, Tablets, etc.) shall be used with reasonable care, as outlined in the **SAO Enterprise Security Policy**.

USE OF STATE TELEPHONES

SAO employees are prohibited from making or charging long-distance telephone calls to SAO, unless for work-related reasons. SAO employees are prohibited from using a State cellular phone for personal calls. However, the receiving and making of local telephone calls of infrequent, short duration are permitted. These privileges may, however, be withdrawn if abused. Voice mail messages should be professional, business-like and should be updated frequently to communicate accurate information.

OTHER EQUIPMENT AND/OR SUPPLIES

SAO employees are responsible for reporting suspected criminal or administrative misconduct regarding misuse of State property to their supervisors, human resource/personnel representatives or other appropriate officials. SAO employees who misuse State property are subject to disciplinary action, up to and including separation from employment.

INAPPROPRIATE USAGE

Inappropriate usage includes (but is not limited to) actual or attempted usage of IT resources for:

- Conducting private or personal for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain;
- Conducting unauthorized not-for-profit business activities;
- Conducting any illegal activities as defined by Federal, State, and local laws or regulations;
- Creation, accessing or transmitting sexually explicit, obscene, or pornographic material;
- Creation, accessing or transmitting material that could be considered discriminatory, offensive, threatening, harassing, or intimidating;
- Creation, accessing, or participation in online gambling;
- Infringement of any copyright, trademark, patent or other intellectual property rights;
- Performing any activity that could cause the loss, corruption of or prevention of rightful access to data or the degradation of system/network performance;
- Conducting any activity or solicitation for political or religious causes;
- Unauthorized distribution of State data and information;
- Attempts to subvert the security of any State or other network or network resources;
- Use of another employee's access for any reason unless explicitly authorized;
- Attempts to modify or remove computer equipment, software, or peripherals without proper authorization;
- Attempts to libel or otherwise defame any person.

DOWNLOADS

Non-approved software, including screen savers, shall not be downloaded or installed from the Internet or other external sources (including portable computing and storage devices) without prior consent from the State agency. Any software that would result in copyright violations shall not be downloaded onto State systems.

HARDWARE INSTALLATION

Hardware devices shall not be attached to a State provided computer that the user does not employ in the user's assigned work. Privately owned devices shall not be connected to State networks, computers (including remotely used computers) or other equipment without approval of the agency prior to connection. All hardware attached to State systems shall be appropriately configured, protected and monitored so it will not compromise State information assets.

PERSONAL USE OF AUDIO CDS, DVDS

State agencies may allow users to play audio CDs or DVDs using State equipment (per State agency policy) provided it does not interfere with their or other's work. Users are not allowed to transfer music from the CD to the workstation or notebook hard drive. Audio CDs that require the user to install software on the workstation or notebook computer may not be played. State agency workstations and notebook computers may not be used to make "compilation" CDs or to "burn" audio or video disks for personal use. State workstation and notebook computers are not be used to transfer music to portable music players. Peer-to-Peer (P2P) file sharing is prohibited on the State network. State agencies shall approve and document any exceptions.

PERSONAL USE OF ENCRYPTION

Personal hardware or software may not be used to encrypt any State or agency owned information so as to deny or restrict access to a public official who has a valid, job-related interest or purpose in the information, except in accordance with express prior permission and direction from the SAO CIO.

PROTECTION OF IT RESOURCES

SAO's information systems are "FOR OFFICIAL USE ONLY". Unauthorized access is a violation of U.S. Law and may result in criminal or administrative penalties. Users will not access other users' or system files without proper authority. Absence of access controls IS NOT authorization for access! SAO information systems and information are intended for communication, transmission, processing, and storage of State of Georgia information. These systems and equipment are subject to monitoring by law enforcement and authorized officials. Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by law enforcement and authorized officials. Use of this system constitutes consent to such monitoring.

- Only use data for which you have been granted authorization.
- Do not retrieve information for someone who does not have authority to access the information; only give information to personnel who have access authority and have a need to know in the performance of their duties.
- Do not access, research, or change any user account, file, directory, table, or record not required to perform your OFFICIAL and authorized duties.
- Do not post SAO information on the internet without prior appropriate permission. Only authorized personnel are allowed to distribute/post SAO information on internet sites (i.e. Blogs, Social networking Sites, message boards, etc)

PROPRIETARY INFORMATION

Proprietary Information should be defined in the policy as any information or data that is created on the company computer system. This information should be construed to become and remains property of SAO. Information received and stored during the normal course of employment should also become property of SAO. Employees should be bound to not disclose any confidential agency information to anyone outside of the agency absent explicit permission from the Chief Information Officer (CIO).

SAO's Proprietary or Confidential Information will remain the sole and exclusive property of the State.

CONSENT TO MONITORING

SAO information technology resources are to be used to conduct official State business. All information created, transmitted, and stored on SAO IT resources is the sole property of the SAO and the State and is subject to monitoring, review, and seizure.

Users of SAO IT resources shall assume NO expectation of personal privacy outside protections provided by the Privacy Act or 1974, HIPAA, and/or other federal, State, or local regulations.

Logging on to any SAO information system is an acknowledgement of this policy and an agreement to abide by it and all other governance regarding its use. SAO has a policy when you log on to the computer of the right and intent to monitor on all computers. SAO may also use filtering software in order to better ensure and/or monitor compliance with this Policy.

ACCOUNTS AND ACCOUNT PASSWORDS

All Users shall be properly authorized and authenticated for use of State of Georgia information assets.

EXCEPTIONS

Exceptions to a policy or standard must be approved by SAO Chief Information Officer (CIO) with review by the SAO Information Security Officer. In each case, the agency or vendor must include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the management approval. Denials of requests for exceptions may be appealed to the State Accounting Officer.

NON-COMPLIANCE

Violations of policy could result in serious security incidents involving sensitive State or federal data. Violators may be subject to disciplinary actions which may include termination and/or criminal prosecution.