



Appropriate Use and Monitoring Policy

State Accounting Office



Table of Contents

PURPOSE..... 4

SCOPE 4

POLICY 4

 NETWORK RESOURCES 4

 INTERNET 5

 EMAIL AND ELECTRONIC COMMUNICATIONS..... 6

 ONE DRIVE FOR BUSINESS 6

 REMOTE LOGIN 6

 OWNERSHIP & CUSTODY 7

 OWNERSHIP 7

 CUSTODY 7

 OTHER EQUIPMENT AND/OR SUPPLIES..... 7

 HARDWARE INSTALLATION..... 7

 PERSONAL USE OF AUDIO CDS, DVDS 7

PROTECTION OF IT RESOURCES..... 8

 CONSENT TO MONITORING 8

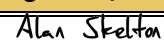

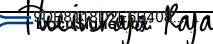

EXEMPTIONS 8

COMPLIANCE 8



Version

Version	Date	Revision / Description	Name
1	11/13/2008	Original Document	Roger Smith
2	4/15/2013	Document Update	Roderick L Wright
3	2/2/2016	Document Update	Mario Covington
4	3/31/2016	Document Update	Mario Covington
5	06/15/2016	Document Update	Patty Pergl
6	09/01/2016	Document Update	Patty Pergl
7	03/09/2017	Document Review	Renee Jones

Name	Role/ Title	Approval For	Approval Signature/ Date
Alan Skelton	State Accounting Officer	Policy	 D62238197A0D4EF... DocuSigned by:
Barbara Rosenke-Sweeney	Chief Information Officer	Policy	 DocuSigned by:
Theinraja Raja	Deputy CIO	Policy	 DocuSigned by:
Renee Jones	Information Security Officer	Policy	 DocuSigned by:



STATE ACCOUNTING OFFICE
Appropriate Use and Monitoring Policy

EFFECTIVE DATE: *June 25, 2013*

RELEASE DATE: *September 1, 2016*

REVISED DATE: *June 5, 2017*

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)
 SAO Remote Access Policy

PURPOSE

The purpose of the Appropriate Use and Monitoring Policy is to define responsibilities and obligations in regards to the usage of Georgia State technology resources. Such usage is subject to State and Federal laws, as well as, Georgia Technology Authority (GTA) and State Accounting Office (SAO) policies and procedures.

SCOPE

The Appropriate Use and Monitoring Policy applies to the State Accounting Office (SAO), including employees, contractors, vendors, external individuals, and organizations.

IT resources for the purposes of this Policy include SAO technology resources owned, managed by, and/or licensed/contracted by SAO. This includes but is not limited to, transmission lines, computer networks, wireless networks, servers, internet connections, terminals, applications, personal computers, and mobile devices, electronic media, computer hardware and software, paper, and telephone systems.

POLICY

SAO IT resources are provided to Authorized Users to facilitate the efficient and effective performance of their duties. It is the responsibility of Users to ensure that such resources are not misused. Following are the Appropriate Use and Monitoring Policy categories.

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. SAO has the right to log the serial #, MAC address, IP of non-State devices connected to the State network, such as personal laptops, jetpacks, wireless access SW/HW, etc.



INTERNET

SAO Employees are responsible for making sure Internet access is used responsibly. Staff should not allow Internet use to interfere with their job duties and responsibilities or otherwise endangering the productivity of SAO. See also *Human Resource Policy: Standards of Conduct, Section 8-Use of State Property* and *Governor's Executive Order, Section 12b-"Personal Use of Telephone and Internet Access"*.

Acceptable Use:

- 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 Use:

- Violation of Federal or Georgia law;
- Infringement and dissemination of copyrighted materials (including articles and software), trademark, patent or other intellectual property rights in violation of copyright laws;
- Conducting private or personal for-profit activities. This includes private business transactions, 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;
- 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.

See also *Human Resource Policy: Standards of Conduct, Section 7-"Activities and Conduct During Working Hours"*



EMAIL AND ELECTRONIC COMMUNICATIONS

Each SAO staff member is given an e-mail account and 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. 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 State information systems or its employees. See also *Human Resource Policy: Standards of Conduct, Section 8-Use of State Property*”.

Specifically prohibited in the use of e-mail is:

- Sending or forwarding any confidential data without encryption.
- Sending, forwarding chain letters, virus, hoaxes, etc.;
- Sending, forwarding or opening executable files (.exe) or other attachments unrelated to specific work activities;
- Submitting any large, unnecessary mail attachments;
- Usage that reflects a non-professional image of SAO such as creation, accessing or transmitting email threads such as jokes or pyramid schemes;
- Sending SAO data, documentation, emails to personal email accounts;
- 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 activity covered by inappropriate usage

ONE DRIVE FOR BUSINESS

SAO has signed an agreement with Microsoft to use Office 365 online for Outlook email services, SharePoint Online, Office Suite, Skype for Business, etc. As part of this agreement, each SAO staff gets 1 TB storage to use OneDrive for Business (ODFB), an online personal storage in the cloud.

- Files on your ODFB should only be synchronized with a SAO issued computer.
- While files on your ODFB storage can be accessed from any computer over the internet, files should not be downloaded to any non-SAO issued computer. All files should be viewed and edited online.
- Files stored in ODFB should not be shared with anyone outside of SAO.
- **No file containing Personally Identifiable Information (PII) data should be stored in ODFB.** Users should review their files stored in ODFB to ensure PII is not contained in any file in their online personal storage. See also [GTA SS-08-002 Classification of Personal Information](#).

REMOTE LOGIN

See also [SAO Remote Access Policy](#), GTA Remote Access Policy [PS-08-023 Remote Access](#), GTA SS-08-038 [Secure Remote Access](#), and GTA SS-08-037 [Teleworking and Remote Access](#).



OWNERSHIP & CUSTODY

OWNERSHIP

- SAO holds the right to possess and transfer custody of the SAO issued Technology Equipment including but not limited to laptops, cell phones, or Jetpacks and its installed software during the Term of this Agreement with the Employee. Personal hardware or software may not be used to encrypt any State or agency owned information 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.

CUSTODY

The Employee is granted rights to use SAO's Technology Equipment during the term of this Agreement subject to all other terms and conditions stated herein. At all times the Employee is responsible for the security, care, custody, and control of the Technology Equipment. The Employee shall not allow unknown or unauthorized individuals to use or access any SAO Technology Equipment. The Employee is responsible for the actions of others while in possession of the Technology Equipment. The Employee will not allow any other person to access his or her network Employee account or password. A SAO laptop that is discovered to be stolen, missing, or damaged must be reported immediately. If criminal activity is suspected with the theft, loss, or damage of an SAO laptop off SAO property, a report must be made to the nearest law enforcement agency. See also [Stolen Laptop Instructions](#)

Helpful HINT: *Take a photo or record your green asset tag number in your phone for future reference*

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. See also *Human Resource Policy: Standards of Conduct, Section 7-"Activities and Conduct During Work Hours"*.

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 to be used to transfer music to portable music players. Peer-to-Peer (P2P) file sharing is prohibited on the State network. State agencies shall document and approve any exception.



PROTECTION OF IT RESOURCES

All Users shall be properly authorized and authenticated for use of State of Georgia information assets. SAO's information systems are proprietary and confidential. 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 authorized duties.
- Do not post SAO information on the internet without prior appropriate permission. Only authorized personnel can distribute/post SAO information on internet sites (i.e. Blogs, Social networking Sites, message boards, etc.)

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 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 may also use filtering software to better ensure and/or monitor compliance with this Policy.

EXEMPTIONS

Exemptions must be approved by the SAO Chief Information Officer (CIO) with review by the SAO Information Security Officer (ISO). In each case, the agency or vendor must complete the [GTA Exemption Request Form](#).

COMPLIANCE

Violation of this policy may result in disciplinary action including termination for employees or termination of employment relations in the case of contractors or consultants. Additionally, individuals would be subject to loss of SAO Information Resources access privileges, and to civil and criminal prosecution. See also *Human Resource Policy: Standards of Conduct: Compliance p.7*