SAO-IT-040	R004	Acceptable Use Policy	08/01/2025
Procedure No.	Rev.	Title	Effective Date
SAO GET Agency Program Manager		DocuSigned by: Stacey Price 32AAF724E6E74BB...	8/5/2025
Approved By		Stacey Price	Approval Date
Director, Digital Services		DocuSigned by: Pamela Woods A1DB3B400C2041...	8/11/2025
Approved By		Pamela Woods	Approval Date
CIO		Signed by: Myra Guy DDD10AA5EA234C0...	8/11/2025
Reviewed & Approved By		Myra Guy	Approval Date
State Accounting Officer		DocuSigned by: Gerlda Hines 996E4838649A4E2...	8/12/2025
Approved By		Gerlda Hines	Approval Date
Annually		***NIST SP 800-53, Revision 5*** *Security and Privacy Controls for Information Systems and Organizations*	
Review Frequency		***GTA SS-08-001*** *Acceptable Use and Monitoring*	
08/01/2026		***GTA PM-04-002*** *Acquisition/Use of Telecommunication Services and Equipment*	
Next Review		***GTA SS-08-009*** *Electronic Communications Accountability*	
Stacey Price		***GTA SS-08-002*** *Classification of Personal Information*	
		GTA SS-08-038 *Secure Remote Access*	
		GTA SS-08-009 *Teleworking and Remote Access*	
		GTA SS-08-011 *Email Use and Protection*	
		SAO-IT-035 *Remote Access Policy*	
		GTA PS-08-023 *Remote Access Policy*	
Agency SME		References	

1.0 Purpose

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

2.0 Scope

2.1 Application to SAO personnel - This policy shall ONLY apply to SAO personnel. This policy does not extend to the users of SAO's information systems that are employed by other State of Georgia agencies. For the purposes of this policy, SAO personnel are defined as employees, contractors, consultants, interns, and individuals who have privileged account access (i.e., Department of Administrative Services (DOAS) Business Analysts, Office of Planning and Budget (OPB) Analytics, etc.). Although, this policy does not govern the behaviors and actions of personnel employed by other State of Georgia agencies or business partners, it does mandate that SAO personnel report activities of these individuals that would in any way represent a compromise or security violation of SAO's information systems. Additionally, while the SAO does not control the specific manner and method (where, when and how) SAO-assigned contractors complete work, these contractors -- like all individuals with direct system access -- are expected to maintain the appropriate level of security awareness to protect SAO system resources. This policy demonstrates separation of duties and applies to the following SAO Personnel, each of which have responsibilities as defined within this policy:

2.1.1 SAO Personnel

2.2 Application to Systems - This policy applies to all SAO agency information systems. Agency information systems include all information systems utilized by personnel of the three divisions of SAO. These information systems include Oracle Financial Consolidation and Close Cloud Service, ERP Application, Travel and Expense System, and any other information system utilized by SAO personnel in support of the mission and operation of SAO. All information that is transmitted or stored on the SAO information systems or SAO IT Resources (including e-mail, files, etc.) is the property of SAO. 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.

3.0 Definitions

Refer to SAO Glossary of Terms and Definitions.

4.0 Exceptions

No Exceptions noted.

5.0 Acceptable Use

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. The following are the Acceptable Use and Monitoring Policy categories.

5.1 Network Resources

5.1.1 SAO employees, vendors/business partners, local governments, and other governmental agencies may be authorized to access State network resources to perform business functions 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 software/hardware, etc.

5.2 Internet

5.2.1 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 endanger 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".

5.3 Acceptable Use

5.3.1 Access to and distribution of information that is in direct support of the business of SAO;

5.3.2 Providing and simplifying communications with other State agencies, State of Georgia employees and citizens of Georgia.

5.3.3 Communication of information related to professional development or to remain current on topics of general SAO interest.

5.3.4 Announcement of new laws, rules, or regulations.

5.3.5 Encouraging collaborative projects and sharing of resources.

5.4 Unacceptable Use

5.4.1 Violation of Federal or Georgia law.

5.4.2 Infringement and dissemination of copyrighted materials (including articles and software), trademarks, patents or other intellectual property rights in violation of copyright laws.

5.4.3 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.

5.4.4 Conducting unauthorized not-for-profit business activities.

5.4.5 Conducting any illegal activities as defined by the Federal, State, and local laws or regulations.

5.4.6 Creating, accessing or transmitting sexually explicit, obscene, or pornographic material.

5.4.7 Creating, accessing, or transmitting material that could be considered discriminatory, offensive, threatening, harassing, or intimidating.

5.4.8 Creating, accessing, or participation in online gambling.

5.4.9 Performing any activity that could cause the loss, corruption of or prevention of rightful access to data or the degradation of system/network performance.

5.4.10 Conducting any activity or solicitation for political or religious causes.

5.4.11 Unauthorized distribution of State data and information.

5.4.12 Attempts to subvert the security of any State or other network or network resources.

5.4.13 Use of another employee's access for any reason.

5.4.14 Attempts to modify or remove computer equipment, software, or peripherals without proper authorization.

5.4.15 Attempts to libel or otherwise defame any person. See also Human Resource Policy: Standards of Conduct, Section 7- "Activities and Conduct During Working Hours"

5.4.16 Attempts to access SAO information systems and Microsoft O365 account from a location outside the United States of America.

5.4.17 Using privileged account to access data in a manner that violates the Need-to-Know Principle. The Need-to-Know Principle limits access to sensitive information to only those individuals who absolutely require it for their specific tasks or responsibilities. In other words, privileged users may have the ability to access data but must not do so unless this access is for mission/business reasons. An example of misuse of access, within the ERP system, may include researching salaries or raises of state employees without having a valid mission/business reason for this access.

5.5 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:

5.5.1 Sending or forwarding any confidential data without encryption.

5.5.2 Sending, forwarding chain letters, viruses, hoaxes, etc.

5.5.3 Sending, forwarding or opening executable files (exe) or other attachments unrelated to specific work activities.

5.5.4 Submitting any large, unnecessary mail attachments.

5.5.5 Usage that reflects a non-professional image of SAO such as creation, accessing or transmitting email threads such as jokes or pyramid schemes.

5.5.6 Sending SAO data, documentation, emails to personal email accounts.

5.5.7 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.

5.5.8 Any activity covered by unacceptable usage.

5.6 One Drive for Business

SAO has signed an agreement with Microsoft to use Office 365 online for Outlook email services, SharePoint Online, Office Suite, 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.

5.6.1 Files on your ODFB should only be synchronized with a SAO issued computer.

5.6.2 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.

5.6.3 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.

5.7 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.

5.8 Ownership and Custody

5.8.1 **SAO Ownership:** SAO holds the right to possess and transfer custody of the SAO issued technology equipment including but not limited to laptops, cell phones 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.

5.8.2 **SAO 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 of the theft, loss, or damage of a SAO laptop off SAO property, a report must be made to the nearest law enforcement agency. See also Stolen Laptop Instructions – Appendix A.

5.9 Other Equipment and/or Supplies

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

5.10 Hardware Installation

5.10.1 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 the 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.

5.11 Protection of IT Resources

5.11.1 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.

5.11.2 Only use data for which you have been granted authorization.

5.11.3 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.

5.11.4 Do not access, research, or change any user account, file, directory, table, or record not required to perform your authorized duties.

5.11.5 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.)

5.12 Consent to Monitoring

5.12.1 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.

5.13 Privileged Account Use and Need-to-Know Principle

5.13.1 Users with privileged access rights (e.g., system administrators, security personnel, application administrators) are strictly prohibited from accessing data or systems beyond the scope of their assigned responsibilities.

5.13.2 All privileged users must adhere to the **Need-to-Know Principle**, which limits access to sensitive or confidential information strictly to those individuals who require such access to perform specific tasks or duties as part of their official role. Possession of elevated access privileges does not constitute authorization to view or use all data accessible through those privileges.

5.13.3 Prohibited activities include, but are not limited to:

5.13.3.1 Accessing personnel or payroll information without a defined and approved business or mission-related justification.

5.13.3.2 Reviewing or retrieving information out of personal curiosity or for unofficial purposes.

5.14 Exemptions

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

5.14.2

5.15 Compliance

5.15.1 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

5.16 Appendix A
Stolen Laptop Instructions

What happens if my laptop is lost or stolen?

1. A SAO laptop that is discovered to be stolen, missing, or damaged, must be reported immediately. (Note: Contact the SAO Internal IT Support team for the asset tag number for your laptop if you do not know it or have access to it).
2. Alert GETS Service Desk team by submitting a ticket through the Service Desk Tool or calling GETS at 1 877-482-3233. Provide the following information:
   - ✓ Employee name
   - ✓ Employee phone number
   - ✓ Employee e-mail address
   - ✓ Laptop asset tag number
   - ✓ What hours the employee works
   - ✓ Time and date of loss
3. Notify the SAO GETS Agency Program Manager and provide them with your GETS Incident #. Notification must occur by submitting a ticket to Internal_IT_Support@sao.ga.gov.
4. If criminal activity is suspected with the theft, loss, or damage of an SAO laptop off SAO property, immediately notify law enforcement and obtain a police report (if applicable)
5. Contact the GETS service desk team and update the original ticket with the police report number (if applicable)

Revision History

Version	Date	Revision / Description	Author
R000	06/30/2021	Initial Version	TeamWorks Policies & Procedures Team: Pam Woods, Melody Richards, Stephanie Starks, Marla Pruitte, Kimberly Williams-Miller, Ethel Hawkins with input from ISO as a Managed Service: Jerry Wyble.
R001	06/30/2022	Updated State Accounting Officer	TeamWorks Policies & Procedures Team: Pam Woods, Melody Richards, Stephanie Starks, Marla Pruitte, Kimberly Williams-Miller.
R002	06/30/2023	Updated Header/Footer and added EZLease and OnSpring systems.	TeamWorks Policies & Procedures Team: Pam Woods, Melody Richards, Stephanie Starks, Kimberly Williams-Miller and Jose Molero.
R003	5/16/2024	Reformatting of the document and added Appendix A: Stolen Laptop instructions.	TeamWorks Policies & Procedures Team: Pam Woods, Stephanie Starks, and Jose Molero.
R004	07/30/2025	Annual updates 2025	TeamWorks Policies & Procedures Team: Pam Woods, Stephanie Starks, Kimberly Williams-Miller, and Ram Reddy Toorpu

SAO
STATE ACCOUNTING OFFICE
200 Piedmont Ave
Atlanta, GA 30335
sao.ga.gov