STATE OF ALABAMA

INFORMATION TECHNOLOGY STANDARD

Standard 660S1: User Rules of Behavior		
Document/Version: 660S1-02	Version Date: 04/09/2021 (draft)	Effective Date: TBD

OBJECTIVE

Define acceptable and non-acceptable use of state-owned information technology (IT) resources including network and Internet access, system and device use, and communications capabilities including email, instant messaging, and social media.

REQUIREMENTS

Section 5 of Chapter 25 of Title 36, Code of Alabama 1975, prohibits public officials or public employees from using their official position or office, including "*equipment, facilities, time, materials, human labor, or other public property under his or her discretion or control for the private benefit or business benefit of the public official, public employee, any other person, or principal campaign committee as defined in Section 17-22A-2, which would materially affect his or her financial interest, except as otherwise provided by law or as provided pursuant to a lawful employment agreement regulated by agency policy*."

The following requirements further define the acceptable and non-acceptable use of state IT resources.

1. INTERNET ACCESS AND USE

1.1. 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 duties. Internet users are expected to handle their access privileges in a responsible manner and to follow all Internet-related policies and procedures.

1.2. 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.

1.3. Users do not have 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.

1.4. 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.

1.5. Agency Head or Agency IT Manager responsibility:

1.5.1. 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.

1.5.2. 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.

1.6. Internet Content Management:

1.6.1. Use of state IT resources for viewing, executing, 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 and liability issues. To mitigate these risks, access to certain categories of Internet content shall be restricted or blocked.

1.6.2. 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 shall therefore be blocked:

1.6.2.1. Games and Gambling
1.6.2.2. Malicious Websites
1.6.2.3. Nudity and Risqué
1.6.2.4. Phishing
1.6.2.5. Peer-to-Peer File Sharing
1.6.2.6. Pornography
1.6.2.7. Proxy Avoidance
1.6.2.8. Spam URLs

1.6.3. Any additional website(s) or category of sites not listed above may also be blocked if deemed a cybersecurity risk.

1.6.4. Exceptions may be granted to access blocked websites for individuals or agencies having a business need for access in order to do their jobs. Each request for access to a blocked website requires a legitimate business need and written approval of the agency head or IT Manager.

2. EMAIL USAGE

2.1. To ensure the integrity and availability of email system resources all electronic communications are expected to comply with relevant federal and state laws as well as state policies and standards.

2.2. Email shall be distributed, stored, and disposed of based on the data content in accordance with state information management requirements or agency Records Disposition Authority.

2.3. Email content created, stored, transmitted, or received using state resources are the property of the state. Authorized personnel may access, monitor, or disclose email content for state business purposes or to satisfy legal obligations.

2.4. Personal use of state email:

2.4.1. State email systems are to be used for business purposes in serving the interests of the government and of the people it serves; non-incidental personal use of state email is prohibited.

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

2.4.3. Personal email shall be deleted or saved separately from work-related email.

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

2.4.5. Users may store personal contact information with their business email contacts.

2.5. State email users are prohibited from:

2.5.1. Creating or distributing 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 email with this content from any state employee shall report the matter to their supervisor immediately.

2.5.2. Sending or forwarding remarks and/or images considered obscene, offensive, racist, libelous, slanderous, or defamatory.

2.5.3. Using an individual state email 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, Senior Agency Information Security Officer (SAISO), or Chief Information Security Officer (unless in the course of normal assigned duties).

2.5.4. Sending unsolicited email 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.

2.5.5. Posting to newsgroups or other social media using a state email address unless in the course of normal business duties.

2.5.6. Using state email for personal or commercial ventures, religious or political causes, endorsement of candidates, or supporting non-government organizations.

2.5.7. Sending or forwarding chain letters or joke email.

2.5.8. Disguising or attempting to disguise the sender's identity when sending email (unless email is sent from a group mailbox).

2.5.9. Sending messages using another person's email account (unless authorized to do so).

2.5.10. Intercepting messages destined for another person's email account (unless specifically delegated access to that person's account).

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

2.6. Auto-forwarding state email: To preclude inadvertent transmission of inappropriate information onto the Internet, auto-forwarding shall not be used to send state email to an Internet, public, or private email address.

2.7. Mass email:

2.7.1. 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.

2.7.2. Message content/format:

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

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

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

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

2.7.3. Message approval:

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

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

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

2.7.3.4. Message shall include a line indicating the state office that approved the mass email.

2.7.4. Message transmission: Mass electronic mailings shall only be transmitted in the evenings (after 5 p.m.) unless immediate notification is required.

2.8. Group Distribution List Owners:

2.8.1. Owners of group distribution lists shall develop and monitor compliance with written operating procedures for the use of their lists.

2.8.2. Owners of large distribution lists shall moderate or otherwise control access to the lists. This applies whether a list has been created for one-time use or is maintained as a standing list.

3. INSTANT MESSAGING

3.1. Instant Messaging (IM) is subject to many of the same threats as email (security flaws, information leaks, vulnerability to malware, etc.), and IM users are frequently the target of phishing attempts.

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

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

3.4. IM file transfers shall be blocked for file transfers external to the organization (in Office 365 this is a global policy set by the tenant administrator).

3.5. IM correspondence 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 and agency record retention policies.

3.6. 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.

4. REMOVABLE STORAGE DEVICES

Removable storage devices (including but not limited to USB flash drives, PC Cards, FireWire devices, MP3 players, camcorders, digital cameras, etc.) could be used to transfer malware to an information system to which they are attached, 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.

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

4.2. 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.

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

4.4. Removable 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.

4.5. Sensitive or confidential data shall not be stored on any removable 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.

4.6. Virus-scan all removable storage devices before device contents are transferred or accessed.

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

4.8. 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.

5. SOCIAL MEDIA

5.1. Organizations may utilize commercial social media platforms (such as Facebook, Instagram, or Twitter) or integrate social media capabilities (such as a wikis or weblogs) into state-hosted websites when beneficial to achieving the business or mission of the agency.

5.2. Organizations shall provide security awareness training to educate users about the risks pertaining to social media and social networking and provide best practices for risk remediation.

5.3. Agency Management Responsibilities:

5.3.1. Agencies shall assess the risk resulting from agency use of social media technologies.

5.3.2. Agencies shall 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.

5.3.3. Agencies must understand that social media contents are public records that must be retained and archived in accordance with applicable agency records disposition requirements.

5.3.4. Agencies shall obtain OIT approval before integrating social media capabilities on any websites hosted, developed, or administered by OIT.

5.3.5. Agencies shall periodically review social media usage to ensure it continues to reflect the agency's communication strategy and priorities.

5.4. Agency IT or Website Administrator Responsibilities:

5.4.1. Site administrator shall disable (if possible) any unnecessary functionality within social media sites or applications, such as IM and file upload/exchange features.

5.4.2. Site administrator shall minimize or eliminate links to other websites to minimize the risk of exposing a government user to a link that leads to inappropriate or unauthorized material.

5.4.3. Site administrator shall suppress any commercial or third-party advertisements (sometimes present when using freeware versions of social media software or tools).

5.4.4. Site administrator shall monitor (and filter as necessary) all social media website content posted or viewed.

5.4.5. Site administrator shall prohibit or block file uploads to the maximum extent possible. Where file uploads are allowed, ensure all user-submitted files are automatically virus scanned.

5.4.6. Site administrator shall include appropriate statements on state-hosted social media sites advising users of the public nature of the information they post.

5.5. Social Media User Responsibilities:

5.5.1. State social media may NOT be used for personal gain, conducting private commercial transactions, or engaging in private business activities.

5.5.2. Users must understand that postings to State social media sites immediately become part of a public record.

5.5.3. Users shall not post or release proprietary, confidential, sensitive, personally identifiable information (PII), or other state government intellectual property on social media sites.

5.5.4. 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.

5.5.5. 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

5.5.6. 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.

5.5.7. 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.

5.5.8. 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.

5.5.9. Users shall use different passwords for different accounts; do not use the same password for both a social media site and state network or email accounts.

5.6. Personal Use of Social Media Site or Application:

5.6.1. 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.

5.6.2. Employees shall NOT use their state email account or password in conjunction with a personal social media site.

6. NETWORK ACCESS AND USE

6.1. Users shall not operate any program, script, command, or send 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.

6.2. Users shall not execute 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 duties.

6.3. Users, including agency information security personnel, shall not conduct network, system, or application scanning unless:

6.3.1. It is within their normal employment responsibilities to conduct such scanning, and

6.3.2. The network, system, or application owner is aware of the scanning activity.

6.4. Users shall not conduct 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.

6.5. Users shall not introduce malicious software (malware) into the network or systems (e.g., viruses, worms, Trojan horses, logic bombs, etc.) within reason of user’s control.

6.6. User shall not access, possess, or transmit material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. STREAMING MEDIA

7.1. Users are permitted to utilize authorized streaming media services (such as YouTube, Vimeo, Microsoft Stream) on state owned devices for approved business purposes to fulfill job duties and responsibilities.

7.2. Users must have supervisor approval prior to uploading or downloading streaming media to ensure it does not distract or impede employee work productivity or consume large amounts of information system resources on state networks.

7.3. Users may access Microsoft Stream media with personally-owned devices by logging into the web portal.

7.4. Users shall not utilize business critical information systems to view, upload or download streaming media on state networks.

7.5. Users shall not upload or redistribute copyrighted material without approval from the copyright owner.

8. DEVICE PROTECTION

8.1. Physical Safeguards:

8.1.1. Whenever leaving a computing device unattended, lock it such that a password or PIN is required to resume use.

8.1.2. Unless kept in a locked room or restricted-access workspace, secure laptops using a cable lock or alarm. Attach the locking cable to an immovable or unbreakable object.

8.1.3 If leaving a device out overnight, lock the entrance(s) to the room. If the room cannot be locked, then secure the device in a locked cabinet or safe.

8.1.4. Eject access card devices and peripheral storage devices from the host system and secure them separately.

8.1.5. Never leave a portable device in view in a vehicle; do not leave devices in a vehicle overnight.

8.1.6. According to the FBI, 97% of unmarked computers are never recovered. Marking the device may increase the chances of having it returned and may also deter casual thieves. Asset tag or engrave the device by permanently marking (or engraving) the outer case or an accessible internal area with the agency name, address, and phone number.

8.1.7. Include a “Return to Sender” text file on any portable devices. This will not deter theft, but it may increase the chances of the device being returned in the event it is found, turned-in for maintenance, or retrieved in the course of an investigation.

8.1.8. For laptops, use a non-descript carrying case rather than a laptop case displaying the manufacturer's logo. Consider using a form-fitting padded sleeve for the laptop and carrying it in a backpack, courier bag, briefcase, or other common non-descript carrying case. Close and lock the zippers of the case so no one can simply reach in and remove the laptop.

8.1.9. Use privacy screens in public facilities or open, high-traffic environments to prevent “shoulder-surfing” when on-screen data needs to be kept private.

8.2. Travel: Public hotspots and wireless networks at airports, hotels, and other establishments present high security risks. Devices using public networks may be scanned by other devices on the network, and information exchanges while connected may be intercepted; therefore, the following protective measures shall be followed.

8.2.1. Do not use open public Wi-Fi unless it is absolutely necessary. Use a VPN (virtual private network) instead.

8.2.2. Use a personal firewall and ensure its settings are set for maximum protection

8.2.3. Upon leaving the public network, immediately restore any security settings that had been disabled and scan the device for viruses and other malware.

8.2.4. Do not download software or applications while on travel unless from a trusted source over a secure channel.

8.2.5. Any device that has been on travel or was connected to an external or un-trusted network shall be checked for compliance with security policies prior to gaining access to state network resources.

8.3. Lost Devices:

8.3.1. Users shall immediately report the loss of any computer or data storage device (including personally-owned devices if used to connect to state networks or store state data) to their immediate supervisor, IT Manager, or Senior Agency Information Security Officer (SAISO).

8.3.2. If possible, Administrators shall perform a remote data wipe to clear the device’s memory.

8.3.3. Because network administrative accounts may have been cached on the device while it was connected to the host network, the System Administrator must change any local network administrative authenticators that may have been used on the lost device.

8.3.4. Recovered devices shall be treated as compromised. Do not connect a previously lost device to any operational network or system until the device has been properly sanitized. There is a significant risk in transferring any user or operational data from the system since there are numerous methods to install and hide malicious code.

SUPPORTING DOCUMENTS

This document is governed by:

- Policy 660: System Use

Additional supporting documents:

- Policy 330: Software Use

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
660S1-01	08/10/2018	Initial version
660S1-02	DRAFT-2104	Removed Software Licensing and Use (moved to Policy 330); requirement 3.4 changed to block external IM file transfers only; edited section 4 for modernization and consistent use of terms; renumbered remaining sections (4.2 to end of requirements); added Section 7: Streaming Media and Section 8: Device Protection, modified supporting documents list, and other format changes.