Mississippi Department of Information Technology Services

3771 Eastwood Drive
Jackson, MS 39211-6381
Phone: 601-432-8000
Fax: 601-713-6380
www.its.ms.gov

David C. Johnson, Executive Director

Appropriate and Acceptable Use of IT Resources Policy

ITS is dedicated to providing the best possible service to customer agencies and is committed to ensuring that the information system resources of the State and ITS are used appropriately for the purposes intended. This policy governs the use of all computers, data and communication networks, and all related software and hardware administered by ITS. A user is defined as any person employed by ITS including fulltime, part-time, temporary, contractors, and any others authorized to use agency information systems. As with all state resources, all information system resources are to be used for state business purposes.

Software

- Software shall not be installed on any desktop, personal computer (PC), or server by anyone other than a representative of the ITS LAN team, without notification to the LAN team via email at LANteamhelpdesk@its.ms.gov. The agency's network contains software that performs an inventory of each PC on a regular basis to ensure compliance with this rule.
- There are to be no games on any desktop, PC, or server at any time for any reason nor games played via web browsers which will be monitored and logged.
- Software owned or licensed by ITS may not be copied to alternate media, distributed by email, transmitted electronically, or used in its original form on any PC other than an ITS PC without express written permission from the LAN team. In no case is the license agreement or copyright to be violated.
- Standard software is to be used for all internal functions and is fully supported by the ITS LAN team. Non-standard software requested by the user and approved by the ITS LAN team is to be used only for required business functions. Unapproved software will be removed by the LAN Team.
- Software licensed to ITS is to be used for its intended purpose according to the license agreement. Employees are responsible for using software in a manner consistent with the licensing agreements of the manufacturer. License agreements are maintained by the LAN team.

Hardware

- Except laptop PCs used for daily offsite work or telework, no equipment should be removed from ITS premises without the permission of the employee's supervisor or Executive Management. Each division has internal guidelines as to how this permission is to be received. In the event equipment is to be off premises for any longer than one work week, the employee responsible for the equipment must file a written hand receipt with the ITS Property Officer (finance@its.ms.gov).
- Laptops, mobile hotspot devices, and other equipment are available for checkout as needed by employees via policies and procedures coordinated by the LAN team.
- In the event that any ITS/State equipment is lost or stolen, employees must notify the ITS Property Officer (finance@its.ms.gov) and ITS LAN team (LANteamhelpdesk@its.ms.gov) immediately for instructions on next steps.

Practices

- System identification codes and passwords are for the use of the specifically assigned user and are to be protected from abuse and/or use by unauthorized individuals.
- Like all ITS information systems resources, internet access, and email are for work-related use. Access and sites visited can and will be monitored at the user level. Each user is

allowed one hour of quota time per day for internet use. ITS email is ITS work product and should be used according to the email use guidelines.

- Employees may not use ITS information systems resources for solicitation, personal financial gain, partisan political activities, or further disseminating "junk" email such as chain letters.
- Information contained on the agency network and workstations is strictly proprietary to the State of Mississippi and ITS. Copying or disseminating any of this information for any purpose other than state business is strictly prohibited. Access to this information must be considered confidential. Access to areas of the LAN is restricted by user ID. Common drives are accessible for collaboration. The H: drive is a personal work area for the employee, while the S: drive is accessible to the division only, and the I: drive is shared agency wide.
- When connecting to the ITS LAN systems with non-ITS computers using VPN and/or VPN/Remote desktop connections, employees are expected to verify that virus definitions are up to date. Information should never be copied or stored on non-ITS equipment including thumb drives. ITS will provide encrypted thumb drives if removable media is required.
- Special attention should be given to encrypt any sensitive data that leaves ITS supported systems.
- Employees are expected to report violations of this policy that is observed to their supervisor or if the violation involves the supervisor to Human Resources or the Chief Administrative Officer. Likewise, if an employee is a witness to a violation, the employee is required to cooperate in any investigation of the violation.
- There may be extenuating circumstances requiring exceptions to this policy including work emergencies, safety issues, etc., that will be reviewed on a case-by-case basis by the Executive Director. This type of review will be the exception and not routine.

Land Based Telephone Usage

- Generally, telephone devices should be used for legitimate state business only; however, brief and occasional personal use is acceptable but should never impede state business. Personal use of the phone system(s) and other land-based telephone devices, where permitted, is a privilege, not a right. As such, use should be limited.
- Confidential information regarding official business should be transmitted from a secure environment. Business facsimile transmissions should include a confidentiality cover notice to limit delivery and distribution.

Wireless Communications

- ITS employees may not directly or indirectly use or allow the use of ITS property of any kind including property leased to ITS for other than state business. In addition, employees shall protect and conserve ITS property, including wireless communications equipment. Wireless communications equipment includes cellular phones, personal digital assistant devices, and standard and two-way pagers, as well as any similar devices that perform some or all of these functions. Employees are hereby notified that ITS will enforce this policy through a variety of methods and may monitor use of wireless communications equipment to assure compliance.
- Employees shall not download, access, or use a prohibited technology on a state-issued device or state-operated network pursuant to the National Security on State Devices and Networks Act (Miss Code Ann. Section 25-53-191). ITS maintains a publicly available list of such prohibited technologies on its website.
- No employee may have more than one wireless communication device assigned and paid for by ITS in compliance with Mississippi Code Annotated, Section 25-53-191. Before a wireless communication device with an active plan is provided to an ITS employee, the Chief Administrative Officer must certify in writing the need for the device and associated service.
- Each employee is responsible for working with their supervisor to determine the most cost-effective communication device and/or service for a given role. Each employee is responsible for reviewing and certifying billings for the device and service utilized and for assessing the need for any change in usage patterns and/or plans based on actual utilization and cost.

- Employees must be aware that cellular phone calling plans are selected based on the number of minutes required for the employee to conduct state business. Package minute plans are not to be construed as free minutes and are not provided for personal use.
- Detailed call billing must be provided for all ITS cellular phone accounts. All billings are considered public records subject to disclosure under the Mississippi Public Records Act.
- Each employee is responsible for verifying their billing details on a regular schedule and indicating by signature that the billing is correct, that all calls were work-related, and that the calling plan is still appropriate to the employee's business needs.
- ITS shall not reimburse employees for any charges on personal wireless communication devices.
- Employees should be aware that cellular phone transmissions are not secure transmissions. Confidential information regarding official business should be transmitted from a secure environment.
- Any ITS employee assigned a wireless communication device must indicate their concurrence with this policy in writing. This written concurrence shall be maintained in the employee's personnel file.

Email Use

The appropriate use of any email sent from an ITS email address applies to all employees, vendors, and others operating on behalf of ITS from the following domains: @its.ms.gov, @its.state.ms.us, @dc.ms.gov or any such domain used for official agency purposes.

- The ITS email system shall be used for electronically conducting official business correspondence.
- No ITS mailbox 'owner' shall allow anyone other than themselves to send mail from their ITS mailbox.
- Employees should keep personal use of the email system to a minimum. All email sent/received or stored by the ITS email system shall become the property of ITS. Sending chain letters or joke emails from an ITS email account is prohibited.
- ITS employees shall have no expectation of privacy in anything they store, send, or receive on the agency's email system. ITS may monitor messages without prior notice, and all messages are considered public records subject to disclosure under the Mississippi Public Records Act unless labeled otherwise by State or ITS attorneys.
- ITS employees shall not set up rules to automatically forward email messages outside of the ITS mail system to personal or other type accounts. Any email forwarded by the user should be for official business only.
- Sensitive data should never be sent via email. This includes data such as Social Security numbers, passwords, and user account information for login to various systems.
- Do not send non-work messages to other ITS employees using groups, mass mailing, or forwarding.
- Do not CC or BCC yourself when sending messages. If you need copies of the messages, please use the built-in message filing capabilities.
- The LAN Team and Human Resources will format signature blocks with an employee's functional title, telephone number, and agency information. Any misspellings or typos should be reported to either the LAN Team or Human Resources asap. No additional information, quotes, etc. should be added to signature blocks and the standard information should not be deleted. Signature blocks are standard for uniformity throughout the agency.
- All email correspondence requiring a response should be responded to within one business day; unless an out of office message is in place to alert senders to the timeframe to expect a reply.
- If an ITS email account will not be checked for more than one business day, the 'owner' of the mailbox must place an out of office message in place to alert senders of the timeframe to expect a reply and who to contact if immediate assistance is necessary.

- ITS mailbox ‘owners’ should remove SPAM immediately from their mailboxes as well as stale messages no longer needed.

Social Media

The *Mississippi State Employee Handbook* provides definitions, guidelines, and reminders regarding personal use of social media by State employees which should be reviewed and adhered to. State email addresses shall not be used to register for personal social media activity.