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
Craig P. Orgeron, CPM, Ph.D., Executive Director

ITS 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 remote work, 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.
- 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 are observed to their supervisor or if the violation involves the supervisor to Human Resources. 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 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 ITS Executive Director or their designee 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.
- 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. While limited incidental use is not prohibited, you should avoid regular personal use and broad distribution
- 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 from their mailboxes as well as stale messages no longer needed in an effort to free up storage resources

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.

Acceptable Use of Artificial Intelligence (AI)

The use of Artificial Intelligence (AI) technologies in ITS operations must be responsible, ethical, secure, and transparent. AI systems—including generative AI tools like ChatGPT—may only be used when approved by ITS and must comply with all relevant laws, privacy standards, and data security protocols. Unauthorized or public AI tools shall not be used with sensitive, confidential, or personally identifiable information (PII), except as otherwise provided in the **Use of Artificial Intelligence Technologies Policy**.

Employees must ensure:

- AI complements, not replaces, human decision-making.
- Outputs are verified for fairness, accuracy, and bias.
- Use of AI is disclosed where appropriate (e.g., public chatbots).
- Only approved platforms are used, with state-issued credentials.
- AI-generated content is reviewed and clearly attributed.

Employees are responsible for understanding and adhering to these guidelines. Requests to use AI shall be directed to your supervisor. Misuse of AI technologies or failure to follow policy may result in disciplinary action. For more details, refer to the full **Use of Artificial Intelligence Technologies Policy** and consult your supervisor. Additional requirements shall be addressed in standards and procedures.

Use of Artificial Intelligence Technologies Policy

This section establishes guidelines for the responsible, appropriate, and secure usage of Artificial Intelligence (AI) technologies, hereafter referred to as “AI systems”, within the State to ensure AI systems are deployed and used in a lawful and ethical manner to enhance productivity and efficiency while complying with applicable legal requirements and respecting privacy, confidentiality, and data security. This policy additionally aims to protect the State's assets, workforce, residents, businesses, and visitors from risks associated with inappropriate use or bias in AI, foster public trust, and support business outcomes. This policy applies to all ITS users (e.g., ITS employees, ITS contractors, guests, stakeholders, etc.) that plan, pilot, develop, acquire, deploy, and/or interact/use AI systems within and/or as part of ITS operations/business. Additional requirements shall be addressed in standards and procedures.

The term "artificial intelligence" has the meaning set forth in 15 U.S.C. § 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action. The term "generative AI" refers to AI that is capable of and used to produce new content, including, audio, code, images, text, and video, according to the data inputs and machine learning model it is trained on.

ITS will maintain a list of AI systems that have been approved for use with specific details regarding which departments/personnel may use each system, what purpose the system can be used for, and data permitted with the system, etc. The list will also include additional safeguards, controls, and processes required. If you are unsure whether a software tool, application, or website employs AI technology and falls within scope of this policy, please contact your supervisor.

General Principles for AI Use

All use of AI systems within ITS must adhere to the following principles:

- **Innovation:** Use of AI should support ITS’s work in modernizing its delivery of services in a more efficient and effective manner as well as help ITS provide improved services and outcomes while also protecting and respecting the privacy, security, and confidentiality rights of all Mississippi citizens.
- **Responsible, Ethical, and Transparent Use:** AI should be used responsibly and ethically to enhance productivity and efficiency in ways that complement human efforts and in a manner that promotes and maintains trust, considers impact, minimizes risks, and maximizes benefits. Elements of transparency include: explainability, traceability, accountability, and openness. Examples include: providing notice to those who may be impacted by AI use; how AI is used to support ITS work/business, disclosure of use of AI in content, interaction with AI versus human; processes/data/decisions made by AI systems are understandable, traceable, and explainable including how systems are trained, what data is used, and provided explanations for automated decisions (where appropriate and ADS permitted); being open/accountable in development and use of AI systems so that all can understand how and why. See additional info in the standards section.
- **Human Oversight and Decision-Making:** Humans must retain control over AI systems, and human decision-makers remain responsible for final decisions made with AI support and/or outputs of AI systems. AI should complement human expertise and judgment, not replace it, and human oversight should be integrated at various stages (as appropriate) to review, refine, or validate AI system results. Automated final decision systems (“ADS”) are not permitted without prior express written approval of ITS as well as additional requirements that must be implemented for high-risk areas. High risk ADSs need to be thoroughly reviewed and assessed prior to use and have multiple levels of safeguards to assess for bias, discrimination, legal compliance, audits, review/monitoring, etc.

- **Fairness and Bias Mitigation:** AI systems must be designed and used ethically, prioritizing fairness. ITS will implement measures to ensure regular monitoring to detect and mitigate biases in data, algorithms, and decision-making processes to avoid discrimination or disparate impact.
- **Privacy and Data Protection:** AI systems/use must respect individual privacy, ensure data protection, comply with all applicable laws and regulations, and preserve individual privacy rights by design. As the use of PII or other non-public data can lead to unauthorized disclosures, legal liabilities, and other consequences sensitive, confidential, or personally identifiable information (PII) must be handled with strict security measures, consent obtained where appropriate and shall not be used with publicly accessible AI systems (e.g., ChatGPT). Additional approval, processes, safeguards, and controls are required for AI systems involving PII/non-public data.
- **Safety and Security:** AI system safety, security, and resiliency must be evaluated to ensure the confidentiality, integrity, and availability of state data. Robust security measures must be implemented to protect AI/ML systems from threats and mitigate AI-related risks. Regular risk assessments, vulnerability assessments, and continuous monitoring are essential and standards addressing resiliency, safety, and security implemented. AI systems must adhere to all applicable ITS and enterprise security policy requirements. Incident response procedures and processes should be expanded to address AI system cybersecurity incidents, findings, mitigations, resolutions, and notification/reporting requirements.
- **Accountability:** ITS and its employees are accountable for the performance, impact, and consequences of AI use. AI systems/use/outcomes must be reviewed/monitored on a regular basis for compliance with all applicable laws, regulations, policies, procedures, standards, guidelines, and best practices. Clear roles and responsibilities should be defined. AI use should also comply with the NIST Artificial Intelligence Risk Management Framework.
- **Accessibility:** AI should be designed and implemented to be inclusive and usable by individuals of all abilities and backgrounds. This includes ensuring AI interfaces are accessible to people with disabilities, providing multilingual support, and reducing barriers to AI adoption for underprivileged communities.
- **Validity and Reliability:** Mechanisms should be in place to ensure systems are working as intended, with accurate outputs, and robust performance.
- **Auditability:** AI systems should be audited and monitored on a regular basis to ensure compliance with applicable laws, regulations, policies, standards, and best practices.

Policy Requirements for the Responsible Use of AI Technologies

Personnel engaged in the use of artificial intelligence (AI) systems or tools must adhere to the following high-level policy requirements. These requirements support ethical, secure, and transparent use of AI in alignment with state laws, enterprise policies, and agency mission.

- **Use of Authorized Technologies:** AI technologies used for official purposes must be sourced from platforms that are approved by the agency or included in the State's enterprise-approved technology catalog once available. The use of any unlisted or emerging technologies shall require prior review and approval by designated officials, such as the Chief Technology Officer, especially in the context of procurement or public-facing applications. Users must coordinate proper approval through their supervisor.
- **Data Governance and Protection:** AI systems must be used in a manner that respects privacy and data protection principles. Users must ensure appropriate approval, oversight, and safeguards are in place before introducing personal, confidential, or regulated data into AI systems to prevent unauthorized access, disclosure, or use of non-public data as well as ensure compliance with applicable legal requirements. Consultation with cybersecurity, privacy, legal officials, and express written approval is required where sensitive data may be involved. Users must safeguard personally identifiable information (PII) and ensure AI tools do not retain or expose sensitive data unintentionally. Data governance procedures and processes related to data availability, quality, integrity, reliability, ownership, access, use, classification, and validation must be in place and any AI data training vetted through appropriate governing processes. Use of AI must comply with applicable data protection and privacy laws, regulations, and guidelines.

- **Human Oversight and Content Accountability:** AI-generated content must not be used as the sole source of truth and shall not be used to solely make decisions for or on behalf of ITS, except as otherwise approved by the agency or included in the State's enterprise-approved technology catalog once available. ITS may use AI to inform a larger decision-making process, but ultimately the responsible user and/or agency remain the final decision maker. Users must review and verify all outputs produced with the assistance of AI. All outputs generated by AI systems are subject to human review to remove bias and validate accuracy, fairness, relevance, and compliance with ethical, legal, policy, and professional standards. Users must maintain editorial oversight to ensure AI-generated materials align with agency values and public trust.
- **Transparency and Attribution:** Where appropriate—particularly in interactions with the public or dissemination of official content—AI-generated output must be clearly labeled or disclosed. Disclosure is required when a user is interacting with a State of MS AI system (i.e. chatbot), and posted options to contact a human are required. Users are responsible for ensuring compliance with applicable intellectual property rights, including appropriate attribution for AI-generated or AI-assisted content, and must consult legal counsel as needed.
- **Risk Awareness and Oversight:** Prior to the adoption of AI systems, ITS and its users must assess potential risks, including cybersecurity, privacy, business continuity, legal, and ethical considerations. Ongoing governance mechanisms must be in place to monitor the performance and impact of AI tools and to identify emerging risks. Users should periodically review AI outputs to ensure continued compliance with reliability, equity, and safety standards.
- **Workforce Readiness:** ITS shall ensure that personnel engaged in AI-related initiatives receive foundational training in responsible and ethical use of AI. Ongoing education should cover AI capabilities, limitations, data classification, and security and privacy implications. Enterprise-wide training programs, including security awareness efforts, should integrate content relevant to AI usage.
- **Compliance and Reporting Obligations:** Use of AI technologies must align with all applicable state and agency-level policies, laws, and regulations. Suspected misuse, security incidents, or policy violations involving AI must be reported through established agency or statewide incident reporting channels. ITS should maintain a clear and auditable process for managing and documenting such incidents.
- **Appropriate Use of Credentials:** All work-related AI activity must be conducted using official state-issued credentials. Personnel are prohibited from using personal email accounts for work-related AI activity. Additionally, access to AI tools must comply with the state's identity and access management protocols, including use of authorized authentication platforms.

Use of AI systems may result in the creation of a public record subject to the Mississippi Public Records Act.

This policy will be reviewed and updated periodically to adapt to the rapidly evolving nature of AI technologies and their implications.