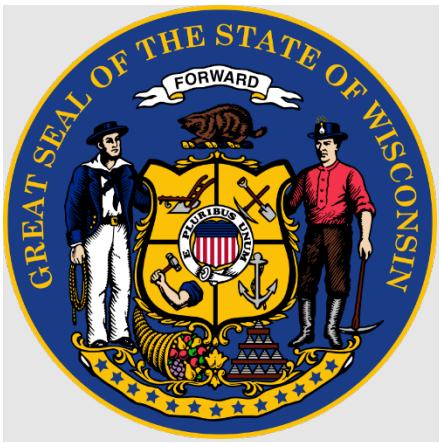

State of Wisconsin – Acceptable Technology Use, Access, and Security Policy

Effective Date: March 10, 2025

Information for Agency IT:

Legal Authority for, and Applicability of, Policy:

Pursuant to the legal authority and mandates set forth in Wis. Stat. §§ 16.971-16.975, the State of Wisconsin Department of Administration (DOA)'s Division of Enterprise Technology (DET), must, among other duties and responsibilities: 1) ensure that information technology (IT) services and resources are available to all executive branch agencies; 2) prescribe policies, standards, procedures, and safeguards for the security and privacy of the information and data contained within those State-managed IT Resources; and 3) ensure that all executive branch agencies develop and operate with clear guidelines. *See, e.g.,* Wis. Stat. § 16.971(2)(a); §§ 16.973(3), (4), and (5); § 16.974(3).

Accordingly, this enterprise-wide Acceptable Technology Use, Access, and Security Policy shall apply to all executive branch agencies, as defined by Wis. Stat. §§ 16.97(5m) and 16.70(4). This shall not apply to the following: Wisconsin Department of Justice, Wisconsin Department of Military Affairs, State of Wisconsin Investment Board, University of Wisconsin System Board of Regents, and the Wisconsin Technical College System Board.

Policy Exceptions:

With respect to the scope outlined in this policy, these are the minimum DET-established policies, standards, and procedures that all executive branch agencies are required to follow. Agency IT Directors are permitted to develop and implement policies, standards, procedures, or requirements for their users that are more stringent than are set forth in this enterprise policy. Agencies that do so should seek guidance and approval from agency legal counsel before developing and implementing those agency policies, standards, procedures, or requirements, to ensure compliance with any laws or standards applicable to the agency's work.

However, agencies are prohibited from developing or implementing policies, standards, procedures, or requirements that directly conflict with this enterprise policy without first requesting and receiving an exception from DET through established DET processes. Before making the request to DET for an exception, agencies are required to receive approval from their legal counsel to ensure the exception can be implemented consistently with the legal requirements applicable to an agency's work.

Questions regarding the risk exception procedures should be directed to the agency's IT Director (through the agency's service request [SR] process or other established IT processes), or to agency legal counsel.

Information for All Users:

Policy Statement:

The State of Wisconsin uses and manages a variety of IT Resources for its operations. Those State-managed IT Resources (as defined below) include, but are not limited to, information, data, equipment, systems, platforms, applications, and facilities. Users' usage of and access to these State-managed IT Resources has significant benefits for the State's operations and for users themselves (*e.g.,* remote/hybrid work), but also can create significant risks to the State, including IT security risks, as well as other legal, operational, audit, privacy, and financial risks.

Therefore, users' use of State-managed IT Resources comes with the expectation that these resources will be used in a manner consistent with stated policies, laws, and regulations. Using State-managed IT Resources in a manner inconsistent with this policy creates liability, security, privacy, and accountability risks which compromise the services that we provide to the public.

Questions about this policy can be directed to the user's supervisor, agency Human Resources, agency IT Director (through the agency's service request [SR] process or other established IT processes), or agency legal counsel.

Scope of Policy:

The responsibilities outlined in this policy apply to all users who are granted rights to access State-managed IT Resources, including all employees and all other non-employee users who are granted rights to use or access State-managed IT Resources through a contractual relationship or other relationship with the State.

A complete listing of authorized State-managed IT Resources, information, equipment, systems, platforms, applications, and facilities is not feasible or desirable, given that technology, data, and access across the State varies and technology rapidly evolves and changes. However, this policy outlines the authorized access and uses of, and applies to, all State-managed IT Resources used in conducting State business.

This Acceptable Technology Use, Access, and Security Policy primarily pertains to policies, standards, and procedures related to State-managed IT Resources, pursuant to DET's statutory authority. However, it also may include references to work rules,

laws/regulations, and other policies. This policy is not intended to supplant, supersede, or replace other policies; users must ensure that they abide by all relevant work rules, laws/regulations, and other policies that are stated elsewhere.

Definitions:

"*Appropriate Security Measures*" means reasonable technical, physical, and procedural controls to protect data against destruction, loss, alteration, unauthorized disclosure, and unauthorized access, whether by accident or otherwise, by employees or other authorized users including contractors. The State of Wisconsin IT Security Policy Handbook has been developed to provide a baseline of executive branch IT security policies and controls, and can be found here: DET Policies, Standards, and Procedures.

"*Artificial intelligence*" (or "AI") means any IT system or part of an IT system able to perform specific tasks that normally require human intelligence. A complete listing of all such technologies or capabilities is not feasible or desirable, but at present includes capabilities such as visual perception, speech recognition, decision-making, creation of new content, documentation and/or data, and language translation.

"*Authorization*" means the security process that an agency uses to determine a user's or service's level of access, as well as legal authority to access. Agencies have staff defined within their organization to determine the appropriate permissions, access privileges, and/or authorizations to access certain kinds of Non-Public Information (as defined below), or to perform particular actions. Users should direct all questions about authorizations, permissions, access privileges, and security processes to their supervisor, agency Human Resources, agency IT Director (through the agency's service request [SR] process), or agency legal counsel.

"*Enterprise Service Desk*" means the 24x7x365 IT support center providing users with a single point of contact for any Division of Enterprise Technology (DET)-managed or supported IT service.

"*Non-Public Information*" means any sensitive or confidential information whose use, dissemination, disclosure, or re-disclosure is protected, restricted, or prohibited from being disclosed by federal or state laws or regulations, or else should be treated confidentially or restricted pursuant to industry standards, policies, and procedures. Examples of "non-public information" include, but are not limited to, personally identifiable information ("PII"), protected health information ("PHI"), student

educational records or information, financial records or information, social security numbers, driver's license information, federal or state tax information, trade secrets, proprietary information, or attorney-client privileged information.

"*PHI*" or "*Protected Health Information*" has the meaning given in Wis. Stat. § 146.816(1)(f) and 45 C.F.R. § 160.103.

"*PII*" or "*Personally Identifiable Information*" has the meaning given in Wis. Stat. § 19.62(5). PII can also include information that, by itself, is not identifying, but when combined with other information could identify a specific individual.

"*Record*" has the meaning given in Wis. Stat. §§ 16.61(2)(b) and 19.32(2).

"*State*" means the State of Wisconsin.

"*State Credentials*" or "Security Credentials" means a proof of identity, such as passwords, biometrics, X.509, digital certificates, key cards, and USB tokens, which control access to information systems.

"*State-managed IT Resources*" include but are not limited to:

- Any State-provided or State-managed information technology device, which may include a computer, computer monitor, fax machine, copy machine, scanner, multi-function device, printer, camera, cellular telephone, tablet, mobile hotspot, or any other State-provided electronic or mobile device which can send, receive, display, or record data, text, pictures, video, or audio through any medium.

- Any State-provided or State-managed e-mail address or other similar State credentials used to access State-managed IT Resources, software, hardware, information system, cloud computing service, social media platforms, other services connected to or hosted on the State network, or other technology provided by the State to a user, or managed by the State, for work purposes.

- The use of voice or data connectivity through any State-provided or State-managed resource, which includes but is not limited to a wired network, wireless network, mobile hotspot, cellular telephone (including voicemail and other

similar Voice over IP [VoIP] systems), remote desktop or virtual desktop, virtual private network, or any other State-provided or State-managed service.

General Usage:

Users of State-managed IT Resources must abide by the following general provisions while using State-managed IT Resources:

- You shall not knowingly or intentionally use State-managed IT Resources to violate any federal, state, or local laws, regulations, or policies, including the State Employee Code of Ethics.

- You shall not use State-managed IT Resources in a manner inconsistent with the terms and conditions governing their use.

- You acknowledge that State-managed IT Resources are constantly monitored by the State for cybersecurity purposes.

- You acknowledge that you have no expectation of privacy associated with the use of State-managed IT Resources. Any information you send, receive, store, or view on State-managed IT Resources is subject to management review and may be monitored, including websites visited and personal communications, both during and outside of work hours.

- You acknowledge that State-managed IT Resources are the property of the State, including all communications sent or received on behalf of the State. As discussed below, all communications sent or received by users are presumed to be public records subject to release under the Wisconsin Public Records Law.

- You may only access data, documents, correspondence, and other records and information that you have been authorized to access and that are necessary to complete your work for the State of Wisconsin.
    - Access to data, documents, correspondence, and other records and information without authorization or for any other purpose is prohibited.

- You acknowledge that all State-managed IT Resources are subject to intellectual property laws, including patents, copyrights, trademarks, and trade secrets, and shall be used in accordance with relevant laws and regulations.
    - When using State-managed IT Resources with content that may be subject to intellectual property protection (*e.g.,* photos, graphics, recordings,

documents, and other information), you must ensure that you have the necessary permission from the owner to use it.

- You shall only communicate using State-managed IT Resources in a manner that is respectful and professional. Harassment, discriminatory conduct, hate speech, and other offensive behavior are prohibited while using State-managed IT Resources.
    - This also applies if you are using State-managed IT Resources to engage on social media, or if you are engaging on social media using a personal device or account in a way that could be attributed to the State of Wisconsin. *See* Wisconsin Human Resources Handbook Chapter 480 (Social Media Usage in State Government) and other applicable enterprise or agency social media policies.

- You are prohibited from using State-managed IT Resources to download, view, solicit, seek, display, or distribute any obscene, pornographic, offensive, or excessively violent material, unless specifically authorized to perform your work responsibilities for the State of Wisconsin.

Regarding Non-Public Information:

Users of State-managed IT Resources acknowledge that the information, data, and knowledge made available for State-related business purposes must be kept safe, and Non-Public Information must be treated as confidential or sensitive. This is necessary to preserve the integrity of State of Wisconsin operations and services.

- You are prohibited from using, disclosing, communicating, or transmitting Non-Public Information without proper authorization, including but not limited to:
    - Copying or transferring Non-Public Information to any form of removable media (*e.g.,* external hard drives, flash drives) without proper authorization.
    - Revealing Non-Public Information on newsgroups, forums, mailing lists, websites, chat rooms, or other similar public/semi-public forums.
    - Accessing or disclosing Non-Public information for any purpose not related to State business, or for any other non-authorized purpose.

- You shall utilize appropriate security measures for all authorized uses, disclosures, communications, transmissions, copies, or transfers of Non-Public Information.
    - You shall immediately contact your agency IT help desk or the Enterprise Service Desk, as soon as you become aware of any suspected or actual unauthorized use, disclosure, communication, transmission, copy, or transfer of Non-Public Information, including the loss or theft of removable media (*e.g.,* external hard drives, flash drives) which may contain Non-Public Information.
    - You must provide this notification even if the unauthorized use or disclosure was inadvertent or accidental. This will allow the agency to determine whether it needs to initiate any legally required mitigation or notification actions, pursuant to each agency's incident response plan. *See* DET's Standard 170 Incident Response Standard.

- You acknowledge that shared files, groups of files, or folders must have proper security configurations, encryptions, and permissions/access rights to comply with legal and regulatory requirements related to Non-Public Information.

- You should avoid disclosing Non-Public Information over text and other non-encrypted or non-secure messaging platforms. Doing so not only creates public records that must be retained and produced, if requested, but may also create unnecessary security and privacy risks.

Public Records and Records Retention:

A comprehensive description of users' public records and records retention obligations is outside the scope of this policy. However, users should assume that any records and other electronic content on State-managed IT Resources (*and* content on personal devices) that are created or being kept in connection with the official purpose or function of the agency are "records" that: 1) should be evaluated by the agency's legal counsel before disclosure to the public, pursuant to the agency's normal public records request processes; and 2) should be retained for the time periods set forth in the applicable General Records Retention Schedule (GRS) or agency-specific Records Retention/Disposition Authorization (RDA).

Users should follow these general records guidelines, in addition to any agency-specific policies or guidelines, to assist in ensuring compliance with public records and

records retention responsibilities and obligations while using State-managed IT Resources:

- The definition of "record" includes but is not limited to electronic records (*e.g.,* emails, Teams chats, text messages), content on virtual platforms (both during meetings and outside of meetings), data, social media content, voicemails, and audio/video recordings, generative AI output, etc., that are created or being kept in connection with State business.
    - If you are using State-managed IT Resources to engage on social media, or if you are engaging on social media using a *personal* device or *personal* account in a way that could be attributed to the State of Wisconsin, you must abide by Wisconsin Human Resources Handbook Chapter 480 (Social Media Usage in State Government) and other applicable enterprise or agency social media policies.

- In addition to applicable records retention schedules, other laws and circumstances may require some records to be retained for longer, such as when a public records request has been made for a record, or if the record pertains to a complaint, investigation, or ongoing litigation.
    - Those retention timeframes may extend beyond the user's period of employment or contractual or other connection with the State.
    - Therefore, before deleting any records, users should consult their supervisor, agency legal counsel, or agency records officer.

Questions about these affirmative records responsibilities, duties, and obligations can be directed to the user's supervisor, agency records officer, or agency legal counsel.

Use of Personal Devices and Personal Accounts:

Users should also follow these general guidelines, in addition to any agency-specific guidelines, to assist in ensuring compliance with public records and records retention responsibilities and obligations:

- You acknowledge that all work-related records (including but not limited to data, communications, pictures, audio, video, or other information) housed on personal *devices* and on personal *accounts* are considered records and are subject to disclosure under the Wisconsin Public Records Law. Such records must also be retained, maintained, and safeguarded per relevant records retention schedules.

- You are encouraged to always use State-managed IT Resources, including State email, Teams, and text messaging on State-issued mobile devices to conduct State business. Doing so will help ensure proper records retention on State-managed IT systems and help protect State-managed IT Resources, information, and data through proper security practices.

- The use of personal *accounts* (*e.g.,* Gmail for emails, personal text messaging *accounts*, and other similar instant messaging-type *accounts* like WhatsApp, etc.) for State business is strongly discouraged. You should not use personal *accounts* to conduct State business, except in very limited circumstances where it is not possible to use State-managed IT Resources.
  - If you use a personal account to conduct State business and create any records using that personal account, you are responsible both for the proper retention of such records, and for making such records available if requested by the public, as well as compliance with any other legal requirements and enterprise or agency policies applicable to the records.
  - With respect to certain types of Non-Public Information (*e.g.,* PII, PHI), the use of personal accounts may also violate other aspects of this policy, other applicable laws or regulations, or enterprise or agency policies. In most instances, users should not use personal accounts to transmit or store Non-Public Information.

- When using personal *devices* or personal *accounts* to conduct State business, you must also ensure that all other security and usage requirements are being met. This includes but is not limited to:
  - Logging into State accounts using State Credentials.
  - Utilizing a secure VPN connection to access State-managed IT Resources when not connected to a State network (*e.g.,* when not connected by state ethernet or Wi-Fi, but when using public or non-secure Wi-Fi).
  - Enabling multi-factor authentication to access Non-Public Information on non-State-issued devices or non-State-managed IT Resources.
  - Not conducting any State business on personal devices or personal accounts using prohibited vendors and technologies, pursuant to DET Standard 290 Removal of Prohibited Foreign Products Standard.
  - Ensuring that any other agency or enterprise policies are followed when using personal devices (*e.g.,* agency Bring Your Own Device policies).

Transcriptions and Recordings:

Information for Agency IT:

Regarding transcriptions and recordings, a comprehensive enterprise-wide policy is neither feasible nor desirable. Each State-managed IT Resource may have its own functionality regarding whether a transcription and/or recording can be made from audio, video, or both (*e.g.,* virtual meetings). Each agency may also have its own needs, policies, and legal requirements regarding permissible uses of transcription and recording functionality. Some transcription and recording functionality may also be enabled by default. Moreover, some State-managed IT Resources may require transcriptions or recordings to be enabled in order to access AI-enabled functionality (*e.g.,* meeting summaries), including AI-enabled functionality that is not yet widely available or not yet in use enterprise-wide. Therefore, agencies are responsible for creating their own policies regarding transcriptions and recordings, and must abide by all relevant DET policies, standards, and procedures if transcription/recording functionality is enabled.

Agency policies must follow all applicable laws, regulations, standards, and procedures to ensure that such recordings or transmissions are not prohibited by law, do not contain Non-Public Information, and do not use Non-Public Information to train a large language model (LLM) contained within AI-enabled technology.

Information for Users:

When deciding whether to transcribe or record a meeting or conversation, users should follow these general guidelines, in addition to any agency-specific guidelines, to assist in ensuring compliance with any applicable laws, regulations, policies, and other requirements related to transcriptions and recordings:

- Unless there is an agency policy expressly permitting such recordings or transcriptions, *and* a business need to record/transcribe, you are strongly discouraged from recording or transcribing any conversations or meetings that occur in audio or video messaging applications, including but not limited to Teams and audio recorders on electronic devices.
    - Transcriptions often contain errors and may not accurately reflect the communication made by the caller or the meeting participant(s).
    - Video and audio recordings are also expensive to retain.

- Before recording or transcribing a meeting or conversation, you must obtain authorization from your supervisor, and you must also notify all attendees or participants that the meeting or conversation is being recorded or transcribed.

- If you have received authorization to record or transcribe meetings, and if such transcriptions or recordings are permissible by agency policy, you must retain the audio/video recording and/or the transcription securely for the relevant records retention period mandated by law.
    - Transcriptions and recordings are distinct records, and both must be retained under relevant records retention periods.
    - Other records created from a transcription and/or recording (*e.g.,* meeting minutes, interview summaries) are also records, and distinct from the transcription/recording. Both should be retained under relevant records retention periods.
    - Transcriptions and recordings are subject to disclosure under the public records law and may be released to the public, if requested.

Users should direct any questions about transcriptions and recordings to their supervisor, agency IT Director, or agency legal counsel.

Closed Captioning:

This transcription/recording policy does not apply to live closed captioning, which may be enabled by anyone during a meeting or call and does not create a record. If a user needs to record or transcribe a meeting as a reasonable accommodation for a disability-related need, please contact your agency's medical coordinator to obtain that accommodation.

IT Security:

The security and safety of State-managed IT Resources is of the utmost importance. In addition to any agency security standards, all users must comply with the following security standards, processes, and practices:

- You should keep all usernames, passwords, multi-factor authentication codes, and other information used to access State-managed IT Resources confidential and never share with others.

    - State of Wisconsin agency IT help desk and Enterprise Service Desk staff will never ask for a user's passwords or codes.
    - If you believe your passwords or codes have been compromised, you should immediately contact your agency IT help desk or the Enterprise Service Desk.

- You shall not use any software, tools, or services that permits another user to remotely access or control another system on any State-managed IT Resource without authorization from your supervisor.
    - This prohibition does not apply to authorized remote access by DET or agency IT personnel for authorized purposes (*e.g.,* help desk).

- You shall not reroute traffic on, scan, probe, or attack a network without authorization.

- You shall not intercept or attempt to intercept any data or other information without authorization.

- You shall not use unauthorized peer-to-peer (P2P) networking, file sharing, instant messaging, or Internet Relay Chat (IRC) applications or services.

- You shall not install or attach any equipment to State-managed IT Resource without your agency's authorization (*e.g.,* wireless access points, modems, disk drives, external hard drives, networking devices, personal mobile devices or computers, monitors, keyboards, mice, printers, etc.). Any unauthorized equipment may be confiscated.
    - This applies to equipment being used, installed, or attached anywhere (*e.g.,* in the office, at home, at remote work location sites, in the community, etc.).
    - For additional information about equipment being used for remote work, *see* Wisconsin Human Resources Handbook, Chapter 748 Remote Work and any applicable agency remote work policies.

- You shall not intentionally modify, damage, repurpose for personal use, or remove State-managed IT Resources without authorization.

- You shall not modify, disable, test, or circumvent any State-managed IT Resource security controls, safeguards, or access controls without authorization.

- You shall not intentionally cause a security incident resulting in a loss of data confidentiality or integrity, or a disruption or denial of availability.
    - This includes using State-managed IT Resources to obtain, or to attempt to obtain, unauthorized access to another computer, to make unauthorized modifications to data, computer programs or supporting documentation, to improperly disrupt the operation of another computer, or to commit any crime.

- You shall not circumvent user authentication or compromise the security of a host, network, or account.

- You shall not compromise, modify, or cause damage to State-managed IT Resources.

- You shall not disrupt or interfere with the normal operation of any State-managed IT Resource.

- You shall not download, install, configure, or modify software or hardware without authorization.

- You shall not store data, records, or other information in public storage services or removable devices, without authorization.

- You shall not use or share any program, disk image, archive, or any form of executable files without authorization.

Suspected Unauthorized Use/Security Incidents:

Users must stop using a State-managed IT Resource when they become aware that it may have been involved in a suspected or actual security incident, data breach, or unauthorized use or disclosure.

- You must use alternative communication methods to report the suspected incident, pursuant to each agency's incident response plan. *See* DET's Standard 170 Incident Response Standard.

- Wait for further instructions prior to doing anything further with the State-managed IT Resource.

- You must not delete anything related to such suspected security incident, data breach, or unauthorized use/disclosure, as such information may legally be required to be kept and/or may assist in a later investigation.

State Credentials/Security Credentials:

Users must take precautions to not disclose information related to State Credentials or Security Credentials. As noted above, users should keep all usernames, passwords, multi-factor authentication codes, and other information used to access State-managed IT Resources confidential and never share with others.

In addition, to prevent information and security compromises, users must adhere to the following:

- Do not provide your State of Wisconsin issued email address, or the email address of other State of Wisconsin employees or contractors, to others on a public forum or while using artificial intelligence (AI) tools without authorization to do so as a State of Wisconsin representative.
  - If you are using State-managed IT Resources to engage in a public forum (including but not limited to social media), or if you are engaging in a public forum using a *personal* device in a way that could be attributed to the State of Wisconsin (including but not limited to using your State of Wisconsin issued email address), you must abide by Wisconsin Human Resources Handbook Chapter 480 (Social Media Usage in State Government) and other applicable enterprise or agency social media policies.
  - If you are using State-managed IT Resources while using artificial intelligence (AI) tools (including but not limited to generative AI tools), or if you are using AI tools using a *personal* device in a way that could be attributed to the State of Wisconsin, you must abide by the requirements for use of AI as stated elsewhere in this policy, along with any other applicable enterprise or agency AI policies.

- Do not re-use passwords from State-managed IT Resources for use on any non-State-managed IT Resources.

- Do not reveal or allow anyone to know or use your State Credentials.

- Do not access State-managed IT Resources with Administrator Credentials or administrator authority unless authorized. If administrator authority is necessary to run an application or perform a task, only approved agency processes may be used to grant that administrator authority.

Workstation/Device Usage:

Users of State-managed IT Resources are expected to keep State-managed IT Resources safe and take all necessary steps to ensure protection from unauthorized use or unauthorized modification, and to ensure that those State-managed IT Resources are maintained within authorized and secure locations.

These State-managed IT Resources are supplied to assist users in providing State services, and as such, must be used and maintained according to this policy and other relevant state and federal laws, policies, regulations, and guidelines. Users must take the following precautions to protect State-managed IT Resources:

- You must lock or log off State-managed IT Resources when unattended.

- Do not use State-managed IT Resources or access State data outside the boundaries of the United States.
    - Use of State-managed IT Resources and access of State data outside the United States is strictly prohibited, except in very limited circumstances and in accordance with DET's International Travel Procedures.
    - International use of State-managed IT resources causes an unacceptable level of cybersecurity risk that in many cases cannot be mitigated.
    - Any use case exceptions for international use must be submitted through DET's risk exception process and pre-approved by both the agency IT director and the agency head before users use State-managed IT Resources outside of United States.
    - This prohibition also includes all State-provided or State-managed IT Resources housed on personal devices (*e.g.,* applications including but not limited to Teams and Outlook).

- Do not bypass or circumvent VPN, firewall, antivirus, or other security measures.

- Non-State Wi-Fi access is inherently not secure, and you should use appropriate security measures when using any State-managed IT Resources that are not connected to a State system or network (*e.g.,* when not connected by state ethernet or Wi-Fi, when using public or non-secure Wi-Fi). Those security measures include but are not limited to:
    - Logging into State accounts using State-provided Credentials.
    - Utilizing a secure VPN connection to access State-managed IT Resources.

- Only devices authorized by your agency may be attached, plugged into, connected with, docked with, paired to, or otherwise provided access to State-managed IT Resources.
    - This includes external hard drives, USB flash drives, memory cards, Bluetooth devices, RFID devices, NFC devices, docks, monitors, keyboards, and mice.

- Removing any State-managed IT Resource other than a State-provided devices, including but not limited to laptops, headsets, webcams, cellular telephone, mobile hotspot, payment processing equipment, or tablet from a user's workspace, including a home office, is prohibited without proper authorization.

- You are responsible for all State-managed IT Resources that have been assigned access and/or issued to you. Damage, loss, or theft of State-issued or State-managed equipment should be immediately reported to your agency IT help desk or the Enterprise Service Desk.

- Repairs to State-issued or State-managed equipment shall be completed only by authorized agency employees, vendors, or contractors.

Personal Use of State-managed IT Resources:

Users of State-managed IT Resources must protect those resources from unauthorized access and misuse. Access is given to assist you in providing State services and to perform State business. To accomplish this, any State-managed IT Resources must only be used in support of approved and authorized State business activities and must not be put at risk by unauthorized access or activity.

Regarding any personal use of State-managed IT Resources, users must abide by the following provisions:

- Do not use State-managed IT Resources for any political or commercial purpose.
    - "Political purpose" is defined in DPM Bulletin DPM-0580-MRS.
    - "Commercial purpose" is defined as any activity for which an employee receives payment or compensation other than through their employment or other contractual relationship with the State of Wisconsin.

- Consistent with State of Wisconsin work rules, you are at all times prohibited from using State-managed IT Resources for engaging in unauthorized activities, including but not limited to gambling, operating a personal business, soliciting, playing games, or any other conduct that is disruptive, decreases the user's productivity, or increases agency costs.

- You acknowledge that any personal use of State-managed IT Resources should be incidental or minimal, including storage of non-work-related files or data on State-managed IT Resources.
    - If you download or store non-work-related files or data on State-managed IT Resources, you must ensure that doing so does not create a security or data privacy risk.
    - It is also recommended that you label any personal files or data housed on State-managed IT Resources, and/or place personal files or data in clearly marked personal folders, especially on shared network drives.

- If using State-managed IT Resources for incidental personal use, you shall not disrupt or interfere with the normal operation of any State-managed IT Resource, including but not limited to causing unnecessary network congestion or application delays within State-managed IT Resources (*e.g.,* streaming video or audio during work hours).

Network Usage:

- Do not bypass or circumvent any State of Wisconsin cybersecurity measure or disrupt the operation of any computer or information system.

- Do not connect any non-State-managed device to a State-managed network unless authorized.

- Do not attempt to bypass State-managed firewalls, routers, or other security systems.

- Do not attempt to access any State-managed IT Resource that you have not been given access to or have not been authorized.

- Do not share any network information such as IP addresses, Wi-Fi passwords, jack location, or other details with anyone unless explicitly requested by approved agency support personnel.

Artificial Intelligence (AI) Usage:

Information for Agency IT:

The State of Wisconsin may seek to use Artificial Intelligence (AI) platforms to leverage their capabilities in gaining unique insights, problem solving, and enhancing productivity at state agencies. It is important to note that each agency and each State-managed IT Resource may have access to its own AI functionality, and needs, policies, and legal requirements regarding its permissible uses of AI technology. AI technology is evolving and developing rapidly; at this time, it is not possible to anticipate all possible uses of AI technology, or risks of those uses.

Therefore, until such time when enterprise frameworks, policies, standards, and procedures are in place, agencies are responsible for creating their own AI policies regarding evaluation and use of AI technology within their agency. Agency AI policies must be reviewed and approved by DOA. Such policies must be consistent with all relevant DET policies, standards, and procedures where AI functionality is enabled or used within State-managed IT Resources. DOA may require agencies to submit additional information, including information from agency legal counsel, as part of the approval process. Once approved, an agency may implement the AI policy to approve AI functionality for purchase and/or use by employees.

Information for Users:

Safeguarding sensitive or confidential information from unauthorized access, use, or disclosure is of utmost importance. Before using AI technology, particularly open-source or publicly available generative AI technology (*e.g.,* Chat GPT, Gemini, etc.), users should review their agency AI policy for any agency-specific requirements. This will help ensure that AI platforms and any associated data handling processes complies with applicable confidentiality and data protection laws and regulations, contractual or legal

obligations. This will also help ensure that the use of AI platforms aligns with existing agency, DET, and enterprise policies that concern but are not limited to data privacy, confidentiality, security, and intellectual property protection. At minimum, users must follow these general guidelines to assist in ensuring safe use of AI and proper compliance:

- You must only use AI platforms and functions that have been authorized for use at your agency and that you have received authorization to use for a specific use case or business purpose.

- You should familiarize yourself and comply with any applicable agency policies, all terms and conditions of the AI platform itself, and any other laws and regulations, including public records and records retention laws.

- You are prohibited from using State Credentials when engaging with AI technology in a personal capacity or on a personal device, unless you have received prior authorization to do so. However, when using an authorized AI tool on State-managed IT resources, you should use your State Credentials to engage with the AI tool.

- You are strictly prohibited from sharing Non-Public Information with any internal or external generative AI platform that has not been authorized for use at your agency.
    - You should be vigilant in using generative AI tools and should report to your supervisor or IT staff the appearance of, or others' unauthorized use of, Non-Public Information in generative AI input or output.
    - You should take care to avoid including specific project details, proprietary information, internal jargon, or any other information that could potentially compromise confidentiality, privacy, or data security, or infringe upon the State's or others' intellectual property rights.

- As a user of State-managed IT Resources, you are responsible for using any AI tools ethically, transparently, and in a manner that minimizes bias and discrimination.
    - Given the known risk of factual errors and algorithmic bias in AI-generated output, you must exercise critical judgment and verify the completeness and accuracy of all information from any AI platform, especially generative AI.

        - You should report to your supervisor or IT staff any erratic or inaccurate behavior of the authorized AI tool.
    - You are prohibited from using AI tools in a way that would violate State of Wisconsin work rules, laws/regulations, and other policies that are stated elsewhere. This includes a prohibition creating or distributing content that is defamatory, discriminatory, malicious, deceptive, or infringes on the rights of others. Any such misuses of AI tools may result in termination of access or disciplinary action.
    - All uses of generative AI and predictive AI must be guided by “human-in-the-loop" principles to ensure that critical thinking and good judgment is exercised. Therefore, you must not deploy an AI output in your work on behalf of the State without conducting an appropriate level of review of such output. For example:
        - If authorized by your agency to create content using generative AI, (e.g., letter or email or memo), you must not use such content without first reviewing and revising it for accuracy, usefulness, and appropriateness of tone and substance;
        - You must not use a generative AI tool to assist with research without conducting independent checks of the content created for accuracy;
        - You must not instruct nor prompt generative AI tools or models to create content in the style of others, and you should clearly attribute any output solely created by AI for State business through a footnote or other means visible to the reader; and
        - Unless using an AI tool expressly authorized by your agency for an expressly authorized purpose, you must not solely use predictive AI for decision-making without also reviewing those predictions, decisions, or outputs, and exercising critical judgment about those predictions, decisions, or outputs.
    - Permissible uses of generative AI may include such uses as brainstorming or generating ideas. If a use case is not included in your agency’s AI policy, or if you are unsure whether a use is permissible, you should ask your supervisor before proceeding.

Internet Usage:

The internet enables users to access and leverage non-State-managed IT Resources, systems, and services, including cloud services. Users of these services must

be cautious and ensure that State security policies are not violated. You must also take the following precautions to protect State interests:

- State agencies have blocked many internet sites that are not appropriate for work purposes.
    - However, you should not assume that a website is appropriate simply because it is not blocked. Certain un-blocked internet sites may also be inappropriate for work purposes or prohibited by other policies.
    - You must abide by all other policies, work rules, and laws related to appropriate internet use.

- Do not use internet services for purposes other than those needed in support of your work duties, with limited, incidental personal use exceptions as outlined by this policy or related agency or enterprise policies.

- Do not share, exchange, transfer, reveal, or otherwise distribute data contained on State-managed IT Resources with any internet site without proper authorization.

- Do not import or download data or information from any internet sources directly into State-managed IT Resources without proper authorization.

- Do not copy, repost, or share information from internet sources unless the source is known, reliable, trustworthy, legal, accurate, public (*i.e.,* not Non-Public Information, sensitive, restricted, or otherwise protected), and properly credited or attributed to the original source.
    - You must also abide by all relevant intellectual property laws when copying, reposting, or sharing information.

Remote Work:

Users of State-managed IT Resources and technology may be allowed or required to work remotely (outside of a State-managed facility). Remote work has many advantages but also creates a unique set of risks and obligations that must be managed to ensure that State-managed systems and data are protected.

Users must abide by all the provisions of this Acceptable Use Policy described herein, as well as applicable human resources policies about remote work, *see*

Wisconsin Human Resources Handbook, Chapter 748 Remote Work and any applicable agency policies.

In addition, users must also take all the following precautions to protect State-managed IT Resources while engaging in remote work:

- The State will provide a computer for employees working from home and may provide other State-managed IT Resources and equipment at its discretion, but you must provision, configure, support, patch, and maintain any personal equipment and services that are needed to enable your remote work.
    - The State will only provide technical support for State-managed IT Resources and will not provide technical support for personal IT equipment and services.
- You must take appropriate steps to secure all State-managed IT Resources and work to prevent unauthorized access or unauthorized use:
    - You shall secure physical documents, lock screens when not in use, and use encryption or password protection for digital files and communications, as required by enterprise or agency policies.
    - You shall not share State-managed IT Resources with unauthorized individuals.
    - You shall not share or disclose Non-Public Information with unauthorized individuals.

Policy Violations:

Users must follow all relevant agency IT policies and procedures, in addition to this enterprise policy. All users must also understand and accept that violating any of these policies exposes the State of Wisconsin to unnecessary risk.

Accordingly, all users must acknowledge that violating any of these policies can constitute work rule violations. The potential consequences for violations include:

- Disciplinary actions, which can include warnings, suspension, or termination of employment, depending upon the severity and frequency of the behavior or violation of work rule.
- Criminal prosecution, if the behavior constitutes a criminal offense.
- Civil liability for behaviors outside the scope of employment.
- Restricted access or termination of access to State-managed IT Resources for users who violate this policy or pose a risk to the security, privacy, and integrity of State systems, networks, or data.