State of Oklahoma
Office of Management and Enterprise Services
Policies and Procedures

Use of Sensitive Data and Systems

Effective date of policy: 03/01/2026	**Next scheduled review: 04/01/2027**
Prior policy:	**Policy number: OMES-042**
Last reviewed:	**Replaces policy number: N/A**
Date policy last revised: 02/09/2026	
Approved: OMES Director Mark Wood	**Approval date: 02/12/2026**

Policy

It is the policy of the Office of Management and Enterprise Services (OMES) that all employees shall access and use agency systems, applications and data only for legitimate business purposes in the performance of their official duties. Employees shall not use their access to sensitive, confidential or nonpublic information for personal interest, personal gain, curiosity or any purpose unrelated to their assigned responsibilities. This includes entering inappropriate or unnecessary prompts into Microsoft 365 Copilot or any similar tool that could retrieve, summarize, analyze or expose data or documents unrelated to the employee's assigned responsibilities. All employees are expected to safeguard the confidentiality of agency data and conduct themselves in a manner that upholds the integrity of the agency's information resources. The policy does not apply to data that is publicly accessible or otherwise available through public means.

Purpose

The purpose of this policy is to establish expectations for the appropriate and lawful use of agency systems, applications, data resources and artificial intelligence (AI) tools, including Microsoft 365 Copilot. This policy is intended to prevent improper access to sensitive, confidential or nonpublic information and to ensure that an employee's access is used strictly for official business in the performance of assigned duties. The policy aims to protect the integrity, confidentiality and security of OMES' information assets and ensure employee access is used solely for official duties, not for personal gain or curiosity.

Scope and Applicability

This policy applies to all agency employees, contractors, temporary staff, interns and any other individual granted access to agency information systems or data resources. It covers access to all nonpublic, sensitive or confidential data maintained, processed, stored or transmitted by the agency. It applies to all systems and mechanisms, including but not limited to human resources information systems (HRIS) (e.g., Workday@OK), case management systems, databases, network storage and any other information systems under the agency's control.

Definitions

1. Sensitive, nonpublic or confidential data means any information restricted by statute, rule, policy or classification. Examples include personally identifiable information, personnel records, financial or benefits information, internal drafts, or information not released under the Oklahoma Open Records Act.
2. Authorized use means using data, systems or tools only to perform official job duties and responsibilities.
3. Unauthorized use means any access, use, query, prompt, viewing or retrieval of data that is not directly tied to the employee's assigned job duties.
4. Publicly accessible data means information that is publicly available. Publicly accessible data is exempt from this policy.

Policy Requirements

Employees may access agency systems only to perform job-related duties. Employees shall not:

1. Browse or explore files, data or folders out of curiosity.
2. Open documents simply because access is available.
3. View personnel, case or program records unrelated to their assigned duties.
4. Access another employee's information without a business need.

Employees shall use Microsoft 365 Copilot and similar tools only for legitimate business tasks. Employees shall not:

1. Enter prompts seeking information they are not authorized to access.
2. Ask Microsoft 365 Copilot to retrieve, search or compile personnel, case or private information.
3. Attempt to circumvent access restrictions through AI prompts or queries.

Employees shall:

1. Protect all sensitive, confidential or nonpublic information learned during their work.
2. Not disclose any sensitive, confidential or nonpublic data to anyone, either inside or outside OMES, without proper authorization.
3. Discuss sensitive, confidential or nonpublic data on a need-to-know basis, but never disclose to anyone outside OMES without proper authorization.
4. Follow all agency confidentiality agreements, security standards and data-handling procedures.
5. Report suspected misuse of systems, data or AI tools.

Disciplinary Action

Violations of this policy may result in disciplinary action up to and including termination.