GOVERNANCE

This document is governed by the IT Governance policy which provides the following requirements:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exceptions and Exemptions
e. Policy Reviews and Updates

SCOPE

This policy covers all State information and systems used, managed, or operated by a contractor, agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and systems supporting the operation and assets of the State.

All information assets that process, store, receive, transmit or otherwise impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy and based on the National Institute of Standards and Technology (NIST) SP 800-53 r5, Configuration Management security controls.

APPLICABILITY

This document addresses the requirements set forth by the State to implement the family of Configuration Management security controls at the organization, process and/or system level for all information assets / State data and provides requirements for the Configuration Management process to assure information systems are designed and configured using controls sufficient to safeguard the State's systems and data.

CM-1 POLICY AND PROCEDURES

The State has adopted the Configuration Management principles established in NIST SP 800-53 r5, "Configuration Management" control guidelines as the official policy for this security domain. The "CM" designator identified in each control represents the NIST-specified identifier for the System and Information Integrity control family. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an Executive Branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The following subsections outline the Configuration Management requirements the State and Executive Branch agencies must implement and maintain for policy compliance.

This policy and associated procedures shall be reviewed and updated at least every three (3) years, unless State-defined events require more frequent review.

This policy and the associated procedures shall be developed, documented, and disseminated by the Agency Head, Chief Information Officer (CIO), Chief Information Security Officer (CISO), or other

designated organizational officials at the senior leadership level.

CM-2 BASELINE CONFIGURATION

The State and Executive Branch agencies shall develop:

a. A current baseline configuration to be reviewed, approved, documented, and maintained under configuration control for each information system. The Office of Information Technology (OIT) shall be responsible for baseline configurations for the enterprise solutions directly provided by OIT.
b. A baseline configuration to document and provide information about information system components of an information system includes but is not limited to:
    i. Standard operating system/installed applications with current version numbers
    ii. Standard software load for workstations, servers, network components, and mobile devices and laptops
    iii. Up-to-date patch level information
    iv. Network topology.
    v. Logical component placement in the system and enterprise architecture
c. New baselines shall be created to reflect information system changes over time to maintain the baseline configuration.
d. Ensure baseline configurations are consistent with the State's enterprise architecture.
e. Use best practices OS hardening baselines.
f. Document baseline configuration exceptions and obtain approval from OIT or designated Agency head.
g. Maintain records confirming baseline configurations separately for each managed system and retain rollback baseline configurations.

Information system configuration baselines shall be reviewed at least annually or more frequently when required for system upgrades, patching, or other significant changes in system security requirements.

CM-3 CONFIGURATION CHANGE CONTROL

Changes to systems and application programs shall be managed to protect them from failure and security breaches. Adequate management of system change control processes requires but is not limited to:

a. Safeguarding production systems during modification, including emergency changes;
b. Enforcement of formal change control procedures;
c. Proper authorization and approvals at all levels;
d. Successful testing of updates and new programs prior to production environment deployment;
e. Determination of the types of changes to the information system that are configuration controlled;
f. Review of proposed configuration-controlled changes to the information system and approval or disapproval of such changes with explicit consideration for security impact analyses;
g. Documenting configuration change decisions associated with the information system;

h. Implementing approved configuration-controlled changes to the information system;
i. Retaining records of configuration-controlled changes to the information system for the life of the system;
j. Auditing and reviewing activities associated with configuration-controlled changes to the information system;
k. Coordinating and providing oversight for configuration change control activities through a Configuration Control Board that convenes when configuration changes occur;
l. Testing, validating, and documenting changes to the information system before implementing;
m. Ensuring updates addressing significant security vulnerabilities are prioritized, evaluated, tested, documented, approved, and applied promptly to minimize the exposure of unpatched resources;
n. Integrating application change control and operational change control procedures, including the following processes, controls, and best practices:
    i. Controls and approval levels for updating libraries
    ii. Requiring formal agreement and approval for any changes
    iii. Restricting library content
    iv. Restricting programmer access to only those parts of the system necessary for their work
    v. Version control for each application
    vi. Tying program documentation updates to source code updates
    vii. Audit logs that track all accesses to libraries, copying and use of source code, and updates posted to libraries.
o. Defining job responsibilities/restrictions and establishing authority levels for:
    i. Developers (should neither test their own code nor promote it into production)
    ii. Other IT staff
p. Identifying personnel authorized to make or submit changes to the source library for each major application to control check-in/check-out;
q. Providing role-based training for business and technical users covering new features and security controls introduced by the upgrade;
r. Using rollback procedures designed to recover to previous stable version of programs.

CM-4 – SECURITY IMPACT ANALYSIS

State/Agency-defined personnel shall conduct a security impact analysis to determine which controls shall be assessed for proper implementation and operation when significant changes are planned and/or made to a system.

Security impact analysis includes but is not limited to reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. The following shall be identified as part of the security risk impact analysis activities:

a. Federal, State, and Local regulatory or legal requirements for the security, confidentiality, and privacy of agency functions or services.
b. Sensitive or Confidential information, and the potential for fraud, misuse, or other illegal activity.
c. Essential access control mechanisms used for requests, authorization, and access approval supporting critical agency functions and services.

d. Processes used to monitor and report to management on whatever applications, tools, and technologies the agency has implemented to adequately manage the risk as defined by the agency (i.e., baseline security reviews, review of logs, use of IDs, logging events for forensics, etc.).
e. Agency change management processes.
f. Security mechanisms to conceal agency data, such as encryption, data masking, etc.
g. Changes potentially impacting security (prior to approval and implementation).

CM-5 – ACCESS RESTRICTIONS FOR CHANGE

The State/Agencies shall define, document, approve, and enforce physical and logical access restrictions associated with changes to information systems and ensure:

a. Only qualified and authorized individuals have access to information system components to initiate changes, including upgrades and modifications.
b. All requests for local administrative rights must be documented and approved by agency management.
c. Access records shall be maintained to ensure configuration change control is implemented as intended and for supporting after-the-fact actions if an unauthorized information system change occurs.
d. Privileges to change information system components and system-related information within a production or operational environment shall be limited to avoid unintended changes to other systems and processes.
e. Use two-person integrity to ensure changes to agency defined critical systems cannot occur unless both individuals implement such changes.
f. Restrict access to operating system and operational or production application software/program libraries to designated staff only.

CM-6 – CONFIGURATION SETTINGS

Configuration settings are parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system.

The State and Executive Branch Agencies shall implement:

a. A standard set of mandatory configuration settings documented for information technologies deployed within the information system. Standard Configuration Documents (SCDs) must detail the configuration settings.
b. The selected configuration settings, whether State standards or designed specifically for the information system, shall reflect the most restrictive mode consistent with operational requirements and be derived from State approved sources.

CM-7 – LEAST FUNCTIONALITY

Agencies shall implement the following requirements to provide least functionality:

a. Information systems provide only essential capabilities and specifically prohibit or restrict functions, ports, protocols, and/or services not required for the business function of the information system.
b. Where technically configurable, the agency will limit component functionality to a single function per device (e.g., email server, web server, etc.).
c. Disable any functions, ports, protocols, and services deemed unnecessary or insecure within an information system.

CM-7 (4) – LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE

The state shall implement the following requirements to provide restrictions on unauthorized software and websites:

a. Identify the types of software programs not authorized to execute on the system and the websites not permitted to be accessed by state-owned equipment;
b. Employ a deny-all, permit-by-exception policy to prohibit the execution of unauthorized software programs and usage of unauthorized websites on the enterprise network; and
c. Review and update the list of unauthorized software programs and websites at least annually.

Unauthorized software and websites can be limited to specific versions or from a specific source. The prohibition on the execution of unauthorized software or usage of unauthorized websites may also be applied to user actions, system ports and protocols, IP addresses/ranges, and MAC addresses. Permitted exceptions to the policy may include usage by law enforcement for investigatory and public safety purposes.

NOTE: OIT has created a "blacklist" outlining the current unauthorized software for all State-owned devices (including mobile devices). The Unauthorized Software List will be maintained as an addendum to this policy specifically for this control enhancement and can be found here - https://oit.alabama.gov/unauthorized-software-list/.

CM-8 – INFORMATION SYSTEM COMPONENT INVENTORY

The State shall update the inventory of information system components as an integral part of component installations, removals, and information system updates, and shall:

a. Develop, document, and maintain an information system component inventory accurately reflecting the current information system environment.
b. Verify all components in the authorization boundary of the information system are not duplicated in other information system component inventories.

Inventory all components within the authorization boundary of the information system (this may include inter-connected systems). This includes information deemed necessary to achieve effective property accountability at the level of detail for tracking and reporting details including, but not limited to:

a. Hardware inventory specifications (manufacturer, type, model, serial number, physical location);

b. Software license information;
c. Information system/component owner(s);
d. Component configuration standards;
e. Software/firmware version information;
f. For a networked component/device, the machine name and network address;
g. Review and audit information system component inventory;
h. Include assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory;
i. Review and update the information system component inventory at least annually.

CM-8 (3) – INFORMATION SYSTEMS COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

Agencies shall employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system, and one or more of the following actions shall be taken:

a. Identify and remove/disable unauthorized and/or non-secure functions, ports, protocols, services, and applications.
b. An information system shall prevent program execution in accordance with agency-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.

CM-9 – CONFIGURATION MANAGEMENT PLAN

The State shall develop, document, and implement a configuration management plan for information systems that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Defines the configuration items for the information system and when in the system development life cycle (SDLC) the configuration items are placed under configuration management;
c. Establishes the means for identifying configuration items throughout the SDLC and a process for managing their configuration;
d. Assigns responsibility for developing the configuration management process to organizational personnel who are not directly involved in system development. In the absence of a dedicated configuration management team, the system integrator may be tasked with developing the configuration management process;
e. Defines detailed processes and procedures for how configuration management is used to support SDLC activities at the information system level;
f. Describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and how documents are developed, released, and updated;
g. Creates a step-by-step implementation plan for every configuration change;
h. Requires that software implementation plans follow change control procedures;
i. Protects the configuration management plan from unauthorized disclosure and modification;

and

j. Requires the configuration management approval process to include designation of key management stakeholders responsible for reviewing and approving proposed changes to the information system, and designation of security personnel that would conduct an impact analysis prior to the implementation of system changes.

CM-10 – SOFTWARE USAGE RESTRICTIONS

The State shall provide employees, contractors and other third parties with guidelines for obeying software licensing agreements including but not limited to open-source software and shall not permit the installation of unauthorized software on devices connecting to State information systems.

Persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties.

Employees, contractors and other third parties shall use software and associated documentation in accordance with contract agreements and copyright laws.

Employees, contractors and other third parties who make, acquire, or use unauthorized copies of software shall be disciplined as appropriate.

Open-source software must:

a. Adhere to a secure configuration baseline checklist from the U.S. government or industry;
b. Inform their users of any proprietary rights in databases or similar compilations and the appropriate use of such data.
c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
d. Establish procedures for software use, distribution, and removal within the agency to ensure software use meets all copyright and licensing requirements. Procedures shall include the development of internal controls to monitor the number of licenses available and the number of copies in use.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

This is the first State of Alabama Configuration Management Policy. All State agencies and vendors of the State are required to comply with the current implemented version of this policy.

REVISION HISTORY

Revision Date	Summary of Change
03/24/2025	New information from Gov. Ivey on restricting access to the sites for TikTok, DeepSeek, and Manus.
01/23/2025	Policy Created

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

APPROVED BY

Signature	Daniel Urquhart
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	03/24/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK