



STATE OF ALABAMA

INFORMATION TECHNOLOGY POLICY



Policy 635: Network and System Access

Document/Version: 635-01

Version Date: 03/15/2021 (draft)

Effective Date: TBD

OBJECTIVE

Manage the granting and rescinding of access to State of Alabama enterprise networks and information systems, plan and utilize appropriate access enforcement mechanisms, and ensure user accountability.

AUDIENCE

Information technology professionals responsible for the granting of network and information system access and management of access control mechanisms.

STATEMENT OF POLICY

This policy defines network and information system access management requirements and responsibilities including access authorization, audit, termination, and enforcement.

It is the policy of OIT that:

- a) Access to state information resources (systems and data) shall be authorized, authenticated, and audited.
- b) Access to state information resources shall be determined by individual information system usage or need-to-know/need-to-share and shall be enforced by appropriate access controls.
- c) Information systems shall employ access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains). [AC-3]
- d) Information systems shall be configured to enforce the most restrictive set of rights, privileges, or access needed by users (or processes acting on behalf of users) as required for the performance of specified tasks (*least privilege*). [AC-6]
- e) Before granting access to a system, display a system use notification or banner informing the user that system and network activities may be monitored, recorded, and are subject to audit by management or other authorized personnel. [AC-8]

AGENCY RESPONSIBILITIES

Information system-owning agencies shall:

- A.1 Develop and maintain an inventory of organizational systems and applications. [PM-5]
- A.2 For each system and application, define and document types of system accounts allowed for use within the system to support organizational missions and business functions. [AC-2a.]
- A.3 Define minimum requirements for information system access control.
- A.4 Assign account managers for system accounts. [AC-2b.]
- A.5 Define (in the system security plan or in agency operating procedures) the specific functions and authority of the account manager role.
- A.6 Require requests to establish network access accounts be approved by a designated account manager, supervisor, or the system owner.
- A.7 Develop procedures to facilitate implementation of this policy and associated access control requirements. [AC-1a.2.]

SUPPORTING DOCUMENTS

The following documents support this policy:

- [Standard 635S1: Access Control Requirements](#)
- [Standard 635S2: Privileged Access Management](#)

AUTHORITY AND APPLICABILITY

This policy is promulgated under the authority granted OIT as described in Policy 101: IT Governance. Unless granted exemption by law or by procedure of Policy 101, the requirements and responsibilities defined in OIT policies apply to all Executive Branch departments, agencies, offices, boards, commissions, bureaus, and authorities and authorized individuals in the employment of or under contract with the State of Alabama and responsible for the management, operation, or use of State IT resources.

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
621-00	09/01/2011	Replaces Policy 620-01 and Standard 620-01S1
621-01	11/23/2011	Modified access termination (revocation and deletion) requirements
635-00	3/15/2021	Number change only
635-01	03/15/2021	Replaces Policy 635-00; completely revised