



KAY IVEY
Governor

STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY



MARTY REDDEN
Acting Secretary

POLICY 635: Network and System Access

VERSION NUMBER	Policy 635-01
VERSION DATE	July 30, 2019
POLICY TITLE	Network and System Access
OBJECTIVE	Manage the granting and rescinding of access to State of Alabama networks and information systems, plan and utilize appropriate access enforcement mechanisms, and ensure user accountability.
AUTHORITY	<p>The authority of the Office of Information Technology (OIT) to create and enforce policies relating to the management and operation of information technology (IT) by state agencies, and exceptions to such authority, are derived from:</p> <p><i>Articles 8 and 11 of Chapter 4 of Title 41, and Chapter 28 of Title 41, Code of Alabama 1975 (Acts 2013-68 and 2017-282).</i></p> <p>Policies of the OIT are approved and signed by the Governor.</p>
APPLICABILITY	The requirements and responsibilities defined in OIT policies apply to all departments, agencies, offices, boards, commissions, bureaus, and authorities (referred to generally as agency or agencies) and authorized individuals in the employment of the State of Alabama responsible for the management, operation, or use of state IT.
STATEMENT OF POLICY	<p>This policy defines network and information system access management requirements and responsibilities to include access authorization, audit, termination, and enforcement.</p> <p>It is the policy of OIT that:</p> <ol style="list-style-type: none"> 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]

OIT
RESPONSIBILITIES

OIT shall:

O.1 Define the minimum standards for information system access control.

O.2 Define the essential functions required of the system account manager role.

O.3 Provide additional guidance for systems processing, storing, or transmitting sensitive or confidential data including but not limited to:

- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Federal Tax Information (FTI)
- Criminal Justice Information (CJI)

AGENCY
RESPONSIBILITIES

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 the types of system accounts allowed for use within the system to support organizational missions and business functions. [AC-2a.]

A.3 Assign account managers for system accounts. [AC-2b.]

- A.4 Define (in the system security plan or in agency operating procedures) the specific functions and authority of the account manager role.
- A.5 Require requests to establish network access accounts be approved by a designated manager, supervisor, or the system owner.
- A.6 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](#)

EFFECTIVE DATE

This policy shall be effective upon its approval by the Secretary of Information Technology and the Governor of Alabama as evidenced by the signatures of the Secretary and Governor being affixed hereto.

SUPERSEDES

This policy supersedes legacy Policy 621: Network & System Access, which is hereby rescinded.

The undersigned, as Acting Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this policy to be adopted as of the date on which the Governor has approved and signed it.

Marty Redden
Acting Secretary of Information Technology

ORDERED

Kay Ivey
Governor

This _____ day of _____, 2019.

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
635-01	07/30/2019	Initial version

DRAFT