



STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY



STANDARD 635S1: Access Control Requirements

VERSION NUMBER	Standard 635S1-01
VERSION DATE	July 30, 2019
STANDARD TITLE	Access Control Requirements
GOVERNING POLICY	This standard is governed by Policy 635: Network and System Access, regardless of revision.
OBJECTIVE	The objective of this standard is to define the basic requirements for system and application access control. There may be additional or more stringent requirements imposed by federal agencies or other regulatory entities. Agencies should consult all applicable sources to ensure compliance with all access control requirements.
REQUIREMENTS	<ol style="list-style-type: none">1. ACCESS CONTROL PROCEDURES Develop, document, and disseminate to applicable personnel procedures to facilitate the implementation of the access control policy and associated access control requirements. [AC-1a.2.]2. ACCOUNT MANAGEMENT<ol style="list-style-type: none">2.1. Account Managers shall:<ol style="list-style-type: none">2.1.1. Establish conditions for group and role membership. [AC-2c.]2.1.2. Specify authorized users of the system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account. [AC-2d.]2.1.3. Require approval by designated agency management (as defined in system security plan or agency operations procedures) for requests to create or modify system accounts. [AC-2e.]2.1.4. Create, enable, modify, disable, and remove system accounts in accordance with agency-defined policy, procedures, and conditions. [AC-2f.]

- 2.1.5. Monitor the use of system accounts; [AC-2g.]
- 2.1.6. Authorize access to the system based on:
 - 2.1.6.1. A valid access authorization;
 - 2.1.6.2. Intended system usage; and
 - 2.1.6.3. Other attributes as required by the organization or associated missions and business functions. [AC-2i.]
- 2.1.7. Review accounts for compliance with account management requirements at a minimum of annually for user accounts and semi-annually for privileged accounts. [AC-2j.]
- 2.1.8. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. [AC-2k.]
- 2.1.9. Align account management processes with personnel termination and transfer processes. [AC-2l.]
- 2.2. Notify account managers as soon as possible:
 - 2.2.1. When accounts are no longer required;
 - 2.2.2. When users are terminated or transferred; or
 - 2.2.3. When individual information system usage or need-to-know changes. [AC-2h.](Agencies may define time-periods for each situation above.)
- 2.3. Default Accounts:
 - 2.3.1. If not needed, default accounts shall be disabled or removed.
 - 2.3.2. Required or active default accounts shall be renamed.
 - 2.3.3. Before deployment in a production environment, default account passwords shall be changed.
 - 2.3.4. Default account passwords shall comply with authentication policy requirements.

3. ACCESS ENFORCEMENT

- 3.1. Information systems shall enforce 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) in state information systems. [AC-3]

3.2. Implement role-based access controls and configure access controls so that each user can access only the pieces of information necessary for the user's role.

4. UNSUCCESSFUL LOGON ATTEMPTS

4.1. Information systems shall enforce a limit of three consecutive invalid logon attempts by a user during a 120-minute period [AC-7a.]; and

4.2. Automatically lock the account for a period of at least 15 minutes unless released by an administrator. [AC-7b.]

5. SYSTEM USE NOTIFICATION (BANNER)

5.1. System use notification message (or banner) shall display, at a minimum, the following information:

5.1.1. That the user is accessing a restricted information system.

5.1.2. That system usage may be monitored, recorded, and subject to audit.

5.1.3. That unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.

5.1.4. That use of the system indicates consent to monitoring and recording. [AC-8a.]

5.2. Retain the notification message or banner on the screen until the user acknowledges the usage conditions and takes explicit action to log on to or further access the information system. [AC-8b.]

5.3. For publicly accessible systems:

5.3.1. Displays system use information when appropriate, before granting further access;

5.3.2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

5.3.3. Includes a description of the authorized uses of the system. [AC-8c.]

6. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

6.1. Identify specific user actions that can be performed on the information system without identification or authentication consistent with agency missions/business functions. [AC-14a.]

6.1.1. Individual accountability requires the ability to trace (audit) the actions of the user who initiated them.

6.1.2. Sensitive and confidential data may not be disclosed to individuals on the information system without identification and authentication.

6.2. Document in the system security plan and provide supporting rationale for user actions not requiring identification or authentication. [AC-14b.]

7. ADDITIONAL REQUIREMENTS FOR MODERATE OR HIGH-RISK SYSTEMS

For moderate or high-risk systems (systems which process, transmit, or store sensitive or confidential information) or systems that require additional access control safeguards (as determined by risk assessment) the following additional requirements shall be applied:

7.1. Automated Account Management:

7.1.1. Employ automated mechanisms to support the management of information system accounts. [AC-2 (CE1)]

7.1.2. Information systems shall automatically disable emergency accounts within 24 hours; and temporary accounts with a fixed duration not to exceed 60 days for moderate risk systems or 30 days for high risk systems. [AC-2 (CE2)]

7.1.3. Information systems shall automatically disable inactive accounts within 60 days for moderate risk systems and 30 days for high risk systems. [AC-2 (CE3)]

7.1.3.1. For systems that process or store FTI, the system shall automatically disable inactive accounts after 120 days of inactivity.

7.1.3.2. RACF shall automatically suspend or revoke inactive accounts after 60 days.

7.1.4. Information systems shall automatically audit account creation, modification, enabling, disabling, and removal actions and notifies defined personnel or roles (as defined in the applicable security plan or agency operating procedures). [AC-2 (CE4)]

7.2. Information Flow Enforcement:

7.2.1. Information flow control regulates where information can travel within an information system and between information systems (as opposed to who can access the information).

7.2.2. Information systems shall enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy or agreements. [AC-4]

7.3. Separation of Duties:

7.3.1. Separate duties of individuals as needed to prevent harmful activity without collusion. [AC-5a.]

7.3.2. Document separation of duties of individuals. [AC-5b.]

7.3.3. Define information system access authorizations to support separation of duties. [AC-5c.]

7.4. Session Lock:

7.4.1. The information system shall prevent further access by initiating a session lock after no more than 15 minutes of inactivity or upon receiving a lock request from a user [AC-11 a.]; and

7.4.2. Retain the session lock until the user reestablishes access using established identification and authentication procedures. [AC-11b.]

7.4.3. The information system shall conceal, via the session lock, information previously visible on the display with a publicly viewable image (e.g., patterns used with screen savers, photos, clock, a blank screen, etc.). [AC-11 (CE1)]

7.5. Session Termination: The information system shall automatically terminate a user session after 30 minutes of inactivity or after other defined condition or trigger event (e.g., response to certain type of incident or time of day restrictions). [AC-12]

SUPPORTING DOCUMENTS

The following documents support this standard:

- [Policy 635: Network and System Access](#)

The following special publication (SP) of the National Institute of Standards and Technology (NIST) supports these requirements and may aid in their implementation:

- NIST SP 800-53R4: Security and Privacy Controls for Federal Information Systems and Organizations

EFFECTIVE DATE

This standard is effective upon its approval by the Secretary of Information Technology, as evidenced by the signature of the Secretary being affixed hereto.

SUPERSEDES

This is the initial standard and does not supersede a previous version.

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 standard to be adopted as of the _____ day of _____, 2019.

Marty Redden
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
635S1-01	07/30/2019	Initial version