



STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY



STANDARD 635S2: Privileged Access Management

VERSION NUMBER	Standard 635S2-01
VERSION DATE	July 30, 2019
STANDARD TITLE	Privileged Access Management
GOVERNING POLICY	This standard is governed by Policy 635: Network and System Access, regardless of revision.
OBJECTIVE	The objectives of privileged access management (PAM) include managing and protecting privileged access channels by associating privileged abilities with specific users, evaluating privileged rights usage, auditing privileged actions, and terminating suspicious actions.
REQUIREMENTS	<ol style="list-style-type: none">1. PRIVILEGED USER ACCOUNTS<ol style="list-style-type: none">1.1. Principle of Least Privilege: allow only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. [AC-6]1.2. Information systems shall employ multi-factor authentication (MFA) for privileged account access.1.3. Agency management shall verify a user requires privileged account access prior to granting it.1.4. Agency management shall ensure that privileged users complete role-based security training before authorizing access to security functions. Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., privileges, permissions), or setting events to be audited. Role-based training is required annually thereafter and when required by information system changes. [AT-3]1.5. Agency management shall review privileged accounts for compliance with account management requirements at a minimum of semi-annually. [AC-2j.]

- 1.6. Privileged user account(s) and all system access shall be disabled or revoked immediately when a user separates from an organization (regardless of reason) or when the account is deemed no longer necessary.
- 1.7. Personnel with privileged user accounts shall not grant elevated privileges to regular accounts without the explicit authorization of agency management.

2. SERVICE ACCOUNTS

2.1. Service accounts are special accounts used by system services (such as web servers, mail transport agents, databases, etc.) to communicate with the operating system (OS). Granting access to a service account to access a resource is similar to granting access to any other identity except that service accounts are very powerful, they run critical system services, and they may bypass some security controls protecting the OS. Because service accounts run with very high, maybe even excessive, privilege, they must be managed like privileged accounts.

2.2. Service Account Best Practices:

- 2.2.1. Create a service account and grant it a role.
- 2.2.2. Name the service account in a manner indicating its purpose.
- 2.2.3. Grant the service account the minimum set of permissions required to achieve its purpose.
- 2.2.4. If a service account is no longer necessary for its intended purpose, disable it.
- 2.2.5. Manage service account passwords and keys.
- 2.2.6. Audit service account activities.

3. 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 audit safeguards (as determined by risk assessment) the following additional requirements shall be applied:

3.1. Least Privilege:

- 3.1.1. Agency management shall explicitly authorize and document approved access to organization-defined security functions and security-relevant information. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for

security services, and access control lists. Explicitly authorized personnel may include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. [AC-6 (CE1)]

3.1.2. Personnel with privileged accounts shall utilize non-privileged accounts to conduct daily business functions when accessing information systems not requiring privileged access. [AC-6 (CE2)]

3.1.3. Agencies shall restrict privileged accounts on information systems to personnel assigned privileged roles (such as system administrator, network administrator, security administrator, etc.), and limit the number of individuals with privileged accounts to that needed to perform such duties and maintain business continuity. [AC-6 (CE5)]

3.1.4. Agencies shall audit the execution of privileged functions on information systems in accordance with audit and accountability policy. [AC-6 (CE9)]

3.1.5. Agencies shall configure information systems to prevent non-privileged users from executing privileged account functions (i.e., creating accounts, installing software, administering cryptographic key management activities, etc.). [AC-6 (CE10)]

3.2. Remote Privileged Access:

3.2.1. Prior to accessing a system remotely, privileged user accounts shall be authorized by agency management for this type of access. Only authorized privileged accounts are allowed to execute privileged commands and have access to security relevant information via remote access. [AC-17 (CE4(a))]

3.2.2. Agencies shall document in their information system security plans justification for privileged user accounts having the capability to access information systems remotely. [AC-17 (CE4(b))]

3.3. Audit Information Protection: Privileged access shall be defined to distinguish between audit-related privileges and other privileges, thereby limiting the number of users with audit-related privileges to a subset of the privileged users. [AU-9 (CE4)]

SUPPORTING DOCUMENTS

The following documents support this standard:

- [Policy 635: Network and System Access](#)
- [Policy 636: Remote Access](#)
- [Policy 645: Audit and Accountability](#)

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
635S2-01	07/30/2019	Initial version