

2.11 Logical Access Security Standard

Effective Date: July 1, 2025

Revised Date: July 1, 2026

1. Purpose

This Standard establishes the mandatory requirements for account creation, management, and information system management across all technology resources and accounts within Arkansas State University (A-State). The purpose of this standard is to ensure that accounts and access controls are managed in a manner that protects university data and mitigates institutional risk.

2. Scope

This standard applies to all faculty, staff, students, contractors, affiliates, and members of the Arkansas State University System (ASU System) community who access A-State information technology infrastructure and associated resources. This standard applies to all institutional platforms and services and applies in all work settings, including on campus, remote work locations, and approved telecommuting arrangements.

3. Definitions

Technology Resources – The machines, devices, systems, services, and related components used in information processing. This includes:

- Machines, devices, and transmission facilities used in information processing, such as computers, word processors, terminals, telephones, cables, software, and related products.
- Devices used to process information through electronic capture, collection, storage, manipulation, transmission, retrieval, and presentation of information in the form of data, text, voice, or image, including telecommunications and office-automation functions.
- Any component related to information processing and wired or wireless telecommunications, including hardware, software, services, planning, personnel, facilities, and training.
- Procedures, equipment, and software designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, along with associated personnel such as consultants and contractors.
- All email accounts issued by A-State.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates,

and members of the system community.

System Community - Any person who accesses the ASU System's IT infrastructure who is not classified as a member of the faculty, staff, or enrolled student.

Systems Authority - ASU System delegates oversight of particular systems to the head of a specific unit of the ASU System or to an individual faculty member, in the case of technology resources purchased with research or other funds for which he or she is personally responsible.

Systems Administrator - A Systems Authority may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular technology resources.

Certifying Authority - This is the Systems Administrator or other ASU System authority who certifies the appropriateness of an official ASU System document for electronic publication in the course of ASU System business.

Specific Authorization - This means documented permission provided by the applicable Systems Administrator.

Privileged Access - Authorized access that allows a user or account to perform administrative or security-sensitive actions on a technology resource that a standard user cannot perform.

Access Control (Logical Access Control) - The administrative and technical measures used to identify and authenticate a user or system and then authorize, enforce, and audit the level of access that identity is authorized for based on least privilege and business need. This includes, but is not limited to, username and password, Multi-Factor Authentication mechanisms, and role or group-based authorization, such as RBAC.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of controls necessary to ensure the effective management and security of digital institutional data. This includes:

Chief Information Officer (CIO) - Responsible for the executive sponsorship, governance, and oversight of the University's information systems management processes within the scope of this standard. Ensures that applicable regulatory, statutory, and contractual obligations are identified, translated into actionable controls, and operationalized across institutional systems and processes.

IT Security Team - Responsible for monitoring the campus' digital infrastructure for both internal and external threats and verification of compliance with organizational objectives and regulatory requirements. This includes the investigation and response of reported or identified security incidents and maintenance of monitoring tools.

ITS Systems Team - Responsible for the campus’ domain-level system administration. Responsible for designing, documenting, maintaining, and overseeing enterprise infrastructure, system configurations, and access to control frameworks. This includes the active management and documentation of all information system accounts.

ITS Endpoint Technicians - Responsible for the management and support of institutional technology resources across the University. This includes the audit and remediation of deployed resources to ensure they comply with standard configuration requirements, the appropriate use of elevated or standard accounts, and the primary support source of technology resource users.

5. Standard Exceptions

The Chief Information Officer is authorized to review and approve exceptions to this standard when organizational needs justify a deviation, and the associated risks are deemed acceptable. All exceptions must be documented, including a defined scope, a scheduled review date, and compensating controls when appropriate. The CIO may delegate this authority as necessary but retains overall accountability for exception management and review.

6. Passphrase Requirements

This section of the standard serves to establish four account security levels and outline their respective passphrase requirements. These account security levels serve to accommodate varying account passphrase requirements based on the sensitivity of systems accessed. Universal account passphrase requirements apply to all security levels unless specified otherwise. This section also outlines requirements for local account passphrases but does not place them at a specific security level as their use outside of emergencies is explicitly restricted.

Account Classification Matrix

Security Level 1 Accounts	Security Level 2 Accounts	Security Level 3 Accounts	Security Level 4 Accounts
Student Accounts	System Administrator Security Level 1 Accounts	System Administrator Accounts	Service Accounts
Faculty Accounts	CJIS User Accounts		
Staff Accounts			
CUI User Accounts			
Shared Accounts (Exception only)			

Passphrase settings are not considered enforced unless systematically required.

6.1 Universal Account Passphrase Requirements

Prohibited Passphrases:

Passphrases must not appear on known compromised passphrase lists or commonly used

passphrase databases. Passphrases will be screened against such lists during passphrase creation and change. A mechanism will be used to detect user passphrases that become compromised after being selected by the user.

Passphrase Reuse:

- A user's passphrase cannot match their last 24 set passphrases within the campus' information systems.
- Users must create unique passphrases for each individual system to which they are given access.
- Reuse of personal account passphrases for business purposes is strictly prohibited.

New User Passphrases:

Users will be required to change their initially assigned passphrase.

Multi-factor Authentication:

Users will be required to authenticate using a multi-factor solution during their first authentication of the day for each individual resource. This authentication will be valid for a period of four (4) hours. Security Level 3 and 4 accounts are excluded from this universal requirement and will instead follow a stricter requirement as outlined in their section.

Alternative Authentication Solutions:

Other technologies for user identification and authentication, such as biometrics, including fingerprint verification or signature verification, and use of hardware tokens, such as smart cards, will be considered and made available for users, if appropriate. Security Level 3 and 4 accounts are excluded from this universal requirement and will instead follow a stricter requirement as outlined in their section.

Duplicated Passphrases:

All user passphrases will be unique and cannot match the passphrase of another account in the campus' information system. This includes any additional account a user may have, such as an administrator account, but excludes accounts synced to the same passphrase using passphrase synchronization at the domain level.

6.2 Security Level 1 Accounts

Passphrase Length:

Account passphrases must be a minimum of 15 characters in length.

Passphrase Complexity:

Passphrases must include at least one uppercase letter, one lowercase letter, one number, and one special character. Repetitive or sequential characters, such as "aaaaaa" or "1234abcd," cannot be present.

Passphrase Rotation:

Account passphrases will expire after a period of 365 days. This expiration will force the user to set a new account passphrase on their next login attempt.

Account Lockout Threshold:

Accounts will be temporarily disabled for 15 minutes after five (5) consecutive failed attempts within a 15-minute period. At the end of this 15-minute lockout, the user's account will automatically unlock, and the process will restart. Passive authentication attempts are excluded from this requirement.

6.3 Security Level 2 Accounts

Passphrase Length:

Account passphrases must be a minimum of 20 characters in length.

Passphrase Complexity:

Repetitive or sequential characters, such as "aaaaaa" or "1234abcd," cannot be present. No other complexity requirements are imposed.

Passphrase Rotation:

Account passphrases will expire after a period of 365 days. This expiration will force the user to set a new account passphrase on their next login attempt.

Account Lockout Threshold:

Accounts will lock after five (5) consecutive invalid logon attempts by a user during a 15-minute period. This account will stay locked until an A-State representative releases the account. Passive authentication attempts are excluded from this requirement.

6.4 Security Level 3 Accounts

Passphrase Length:

Account passphrases must be a minimum of 20 characters in length.

Passphrase Complexity:

Repetitive or sequential characters, such as "aaaaaa" or "1234abcd," cannot be present. No other complexity requirements are imposed.

Passphrase Rotation:

Account passphrases will expire after a period of 365 days. This expiration will force the user to set a new account passphrase on their next login attempt.

Account Lockout Threshold:

Accounts will lock after five (5) consecutive invalid logon attempts by a user during a 15-minute period. This account will stay locked until an A-State representative releases the account. Passive authentication attempts are excluded from this requirement.

Enhanced MFA Requirements:

Users will be required to authenticate using a multi-factor solution upon each account authentication.

Technology Resource Configuration:

Technology resources will be configured to restrict Security Level 3 accounts from direct access. Instead, privileged access shall be granted via elevation from a Security Level 2 account using system-specific solutions, such as Sudo or RunAs.

6.5 Security Level 4 Accounts

Passphrase Length:

Account passphrases must be a minimum of 30 characters in length.

Passphrase Complexity:

Account passphrases must be sufficiently complex and resistant to brute-force or dictionary attacks. Use of randomly generated passphrases is required.

Passphrase Rotation:

Account passphrases will expire after a period of 730 days. If an employee who has accessed a Security Level 4 account leaves the organization, this passphrase will be reset.

Passphrase Access:

Security Level 4 account information will be stored in a single passphrase management system. Access to passphrases in this system by administrators must be logged with access logs retained for a minimum of three years.

Early Passphrase Rotation:

When an employee who has accessed a service account leaves the organization, that Security Level 4 account passphrase must be reset within 12 hours of the employee's account being disabled. A passphrase reset of this nature will be considered an emergency priority for change management purposes.

7. Local Accounts

In alignment with the A-State Technology Resource Management Standard, local accounts will be restricted as follows:

7.1 Local Account Passphrase Requirements

Technician Generated Accounts

- Local user or administrator accounts created by either endpoint technicians or systems administrators for specific use cases will have their passphrases changed every 60 days. Passphrase age will be tracked within an EDR when available to ensure compliance.
- Account passphrases will be a minimum of 25 characters with at least one uppercase letter, one lowercase letter, one number, and one special character.
- Local user or administrator accounts created by either endpoint technicians or ITS Systems Team must be documented and have an approved CIO exception on file.
- Local user or administrator accounts, other than a system-generated default administrator account, will not be permitted on endpoints in areas such as the University Police

Department, Information and Technology Services department, the University Data Center, and any other area containing Regulated or Confidential data as classified by the Data Security and Classification Policy.

7.2 Local Administrator Privileges

- Standard users shall not have standing local administrator rights.
- Privileged access shall be limited to authorized A-State ITS personnel.
- Authorized privileged access shall not be granted via the use of static local accounts and will instead utilize an approved privileged access management (PAM) solution, such as Microsoft Local Administrator Password Solution (LAPS). Upon use, this password will automatically be regenerated.

8. Passphrase Enforcement and Monitoring Controls

A-State shall maintain a supplemental Logical Access Password Enforcement and Monitoring Procedure, separate from this standard, that outlines the technical controls ITS utilizes for password enforcement and password compliance ensuring this monitoring is maintained in accordance with state, federal, and university regulations and policies. At a minimum, this will include and establish the following subjects:

- How Fine-Grained Passphrase Policies (FGPP) are configured to ensure compliance with this standard.
- How passphrase complexity and length requirements are configured to ensure compliance with this standard.
- How Entra passphrase protection for Active Directory is configured for both on-premises and cloud-based accounts in compliance with this standard.
- How CrowdStrike compromised password workflows are configured to ensure compliance with this standard.

9. Access Management Requirements

To ensure compliance with university standards, the ITS Systems Team will maintain, support, and centrally administer user accounts with the institutional goal of reducing operational and cybersecurity risk. The ITS Systems Team shall maintain a supplemental Logical Access Account Management Procedure, separate from this standard, that outlines how these resources are configured, monitored, and managed.

This procedure will, at a minimum, include and establish the following requirements:

- All user accounts will follow a defined and documented naming scheme.
- Shared accounts are not permitted for access to A-State information systems. Though “shared” by administrators, service accounts are not considered shared accounts for the purposes of this requirement.
- All service accounts will be thoroughly documented by the ITS Systems Team, with purpose and any automated tasks executed defined.

- Information system accounts will be created so that they enforce the most restrictive set of rights, privileges, or accesses required for the performance of tasks associated with their assigned job duties.
- Information system accounts with rights, privileges, or accesses extending into the administrative management of endpoints, information systems, or other technology resources will result in an administrative account being created for the user. This administrative account will exist solely for the completion of assigned job duties extending beyond that of a standard user account.
- All information system accounts will be actively managed. Active management includes the acts of establishing, documenting, activating, modifying, disabling, and removing accounts from A-State's information systems. This work will be completed by a domain-level system administrator.
- Timelines and requirements for the timely disablement of accounts when their assigned user is no longer employed or associated with the organization.
- Information system accounts are to be reviewed by the ITS Systems Team to verify access is still relevant to their assigned duties.

Review will include verification of:

- Continued business justification for access.
- Confirmation of appropriate role-based group membership.
- Any access that is no longer justified must be revoked within one (1) business day of the review.

10. Access Management Controls

Management of A-State access controls shall meet the following requirements:

- Access to information system resources will be logged and stored for a minimum of seven (7) years unless otherwise specified in the University Data Retention Procedure. Suspicious access will be reported to the Security Team for evaluation.
- Service account usernames and passphrase information will be stored, transmitted, and tracked using a single passphrase management solution. Account information is not permitted for transmission via any other form of communication.
- Service account passphrases shall be rotated within 24 hours of the receipt of the termination workflow for any user(s) that have accessed the service account.
- The ITS Systems Team will create adequate documentation of the account management processes, tools, workflows, and mechanisms required to actively maintain A-State access management controls.

11. Use of Access Controls

Arkansas State University invests substantial and sufficient resources to acquire and operate information technology assets, such as hardware, software, and Internet connections. ITS has a responsibility to manage its resources in the most efficient and effective manner possible and in compliance with all laws, regulations, and sound business practices, while at the same time

protecting and preserving the right to academic freedom. Effective management of these resources will assure students, faculty, and staff adequate access to information and technology over the long term and ensures compliance with Arkansas State University System policy. Examples of appropriate and inappropriate uses of access controls include, but are not limited to, the following:

Appropriate Use of Access Controls

- Users only use their assigned user account for access to A-State resources.
- Users only use their assigned authentication methods, such as MFA, to access A-State resources.
- Using university-approved password management solution(s) to store access control information.
- Reporting observed violations of this Logical Access Security Standard.

Inappropriate Use of Access Controls

- Sharing access credentials such as passwords with another user.
- Sharing authentication methods such as access to MFA mechanisms with another user.
- Providing inappropriate access to another user in violation of the principle of least privilege.
- Writing access control information outside of a secure, university-approved password management solution.

12. Standards Review

This document will be reviewed and reaffirmed annually, or upon significant changes to university IT governance, systems, or regulatory requirements.

Effective Date: July 1, 2025

Next Review Date: July 1, 2027

Version: 2.0

Referenced Policies, Standards, and Procedures

- Technology Resource Management Standard
- Data Security and Classification Policy
- Arkansas State University Data Retention Procedure
- Logical Access Account Management Procedure
- Logical Access Password Enforcement and Monitoring Procedure

Revision #11

Created 2025-10-02 01:52:54 UTC by Christopher Boothman

Updated 2026-07-07 17:21:05 UTC by Jacob Weaver