
	Identification and Authentication Policy		
PR-AA-P3			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 1 of 9

GOVERNANCE

This document is governed by the IT Governance policy which provides the following requirements:

- a. Roles and Responsibilities
- b. Policy Control Application
- c. Policy Compliance Requirements
- d. Policy Exceptions and Exemptions
- e. Policy Reviews and Updates

SCOPE

This policy covers all State information and systems used, managed, or operated by a contractor, agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and systems supporting the operation and assets of the State.

All information assets that process, store, receive, transmit or otherwise impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy and based on the National Institute of Standards and Technology (NIST) SP 800-53 r5, Security and Privacy Controls.

APPLICABILITY

This document addresses the requirements set forth by the State to implement the family of Identification and Authentication security controls at the organization, process and/or system level for all information assets/State data and provides requirements for the identification and authentication process to assure information systems are designed and configured using controls sufficient to safeguard the State's systems and data.

IA-1 POLICY AND PROCEDURES



The State has adopted the Identification and Authentication principles established in NIST SP 800-53 r5, "Identification and Authentication" control guidelines as the official policy for this security domain. The "IA" designator identified in each control represents the NIST-specified identifier for the Identification and Authentication control family. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an executive-branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The following subsections outline the Identification and Authentication requirements the State and executive-branch agencies must implement and maintain for policy compliance.

This policy and associated procedures shall be reviewed and updated at least every three (3) years unless State-defined events require more frequent review.

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATION USERS)

Information systems shall be configured to uniquely identify and authenticate users, devices, or

	Identification and Authentication Policy		
PR-AA-P3			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 2 of 9

processes acting on behalf of users.

Access to information systems is defined as either remote, local, or network access. Local access is any access to information systems by users, devices, or processes acting on behalf of users connecting directly without the use of networks.

Network access is access to information systems by users, devices, or processes acting on behalf of users obtained through network connections.

System owners shall not allow the use of shared accounts (credentials used by more than one individual) within their system. The use of shared user accounts makes it difficult to uniquely identify individuals accessing an information system, as well as provide detailed accountability of user activity within an information system.

Identification and authentication mechanisms shall be implemented at the application level, as determined by a risk assessment, to provide increased security for the information system and the information processes. This shall be in addition to identifying and authenticating users at the information system level (i.e., when initially logging into a desktop, laptop, or mobile device). Single sign-on is permitted only after authentication into the network.

Access to all non-privileged, privileged, and local accounts shall be authenticated with unique identification and password. Note: See IA-5 - Authenticator Management for password complexity requirements and definitions of privileged and non-privileged accounts.

Multi-factor authentication (MFA) shall be implemented for all network access and shall be such that at least one of the factors is provided by a device or control separate from the device used for access. MFA shall consist of two or more of the following:

- a. Something the user knows (e.g., a password or personal identification number);
- b. Something the user has (e.g., a hard- or soft-token); and
- c. Something the user is (e.g., biometric identification).

IA-2 (1) IDENTIFICATION AND AUTHENTICATION | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

MFA shall be implemented for all privileged account access.

IA-2 (2) IDENTIFICATION AND AUTHENTICATION | MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS



MFA shall be implemented for all non-privileged account access.

IA-2 (8) IDENTIFICATION AND AUTHENTICATION | ACCESS TO ACCOUNTS – REPLAY RESISTANT

Information systems shall implement replay-resistant authentication mechanisms for network access to privileged or non-privileged accounts if technically configurable.

IA-2 (12) IDENTIFICATION AND AUTHENTICATION | IDENTIFICATION AND AUTHENTICATION PROOFING

Organizations shall require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines.

	Identification and Authentication Policy		
PR-AA-P3			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 3 of 9

Organizations shall accept and verify different authentication types through hardware and software tokens specifically proving the identity of the users.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Users accessing State resources from personal devices shall adhere to the required security configurations, including but not limited to, current patches and anti-virus files on those devices. Additionally, State or executive-branch agencies will ensure that:

- a. Procedures verifying node authentication measures shall be developed;
- b. Only approved procedures, mechanisms, or protocols shall be used for host or device authentication; and
- c. Network routing controls should be implemented to supplement equipment identification by allowing specific equipment to connect only from specified external networks or internal sub networks (“subnets”).

IA-4 IDENTIFIER MANAGEMENT

All State information systems, including cloud-based services, shall:

- a. Receive authorization from a designated State or executive-branch agency representative (e.g., system administrator, technical lead, or system owner) to assign individual, group, role, service, or device identifiers;
- b. Select and assign information system identifiers to uniquely identify an individual, group, role, service, or device. Assignment of individual, group, role, service, or device identifiers ensures no users or devices have the same identifier;
- c. Avoid reuse of identifiers for an agency-defined timeframe and management may allow limited reuse in exigent circumstances;
- d. Disable identifiers after 90 days of inactivity, except as specifically exempted by agency management. Identifiers should be disabled immediately upon dismissal, notification, or upon request; and
- e. Disabled Identifiers with no activity after 90 days should be deleted, but retention should remain for an agency-defined timeframe. Identifiers should be disabled immediately upon notification of request.



IA-4 (4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS

Procedures shall be implemented ensuring individual identifiers are managed by uniquely identifying the user’s credentials, such as employee, contractor, active, inactive, lock, or disabled.



IA-5 AUTHENTICATOR MANAGEMENT

Information system authentication requirements shall be managed. Individual authenticators include, but are not limited to, passwords, tokens, biometrics, PKI certificates, and key cards. The following items are required:

- a. Develop secure log-on procedures for all network components, operating systems, applications, and databases with a user identification and authentication mechanism.
- b. Initial authenticator (password) distribution requires confirming the identity of the individual, group, role, service, or device receiving the authenticator.

	Identification and Authentication Policy		
PR-AA-P3			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 4 of 9

- c. Establish initial authenticator content for authenticators issued by the State (e.g., default passwords).
- d. Change all default passwords immediately after system install. Require all users to change the default password immediately after initial login or after a password reset.
- e. Ensure sufficient strength of mechanism for authenticators. All passwords must meet the following composition and complexity requirements:
 - i. Be at least eight (8) characters and contain a combination of at least one (1) number, uppercase letter, lowercase letter, and special character. The use of passphrases is encouraged to create longer passwords. Agencies with more stringent regulatory compliance requirements based on data type will follow that prescriptive guidance. If passphrases are used, spaces are considered special characters.
 - ii. Passwords shall not contain number or character substitutes to create dictionary words.
 - iii. Change at least one (1) character when passwords are updated.
 - iv. Password lifetime restrictions shall be at least a one (1) day minimum and no more than 90 days maximum.
 - v. Service account passwords must be updated after 365 days (366 days inclusive).
 - vi. Require at least 24 generations before a password may be reused. For systems unable to implement history/reuse restriction by generation, but can restrict history/reuse by time period, passwords shall not be reusable for at least six (6) months.
- f. Establish and implement administrative procedures for authenticator:
 - i. Distribution
 - ii. Loss
 - iii. Compromise
 - iv. Damage
 - v. Revocation
- g. Users must implement specific security safeguards to protect authenticators from unauthorized disclosure and modification.
- h. Change authenticators for group/role accounts when membership changes.
 - i. Information systems shall display a message to users before or during prompts for identification and authentication credentials warning against unauthorized or unlawful use. (Such as a System Use Notification Banner)
 - j. The log-on process shall not be validated until all log-on data is completed.
- k. Only generic “log-on failed” messages should be displayed if the user does not complete the log-on process successfully without identifying if user identification, password, or other information is incorrect.
 - l. Systems shall be configured to limit the number of consecutive unsuccessful log-on attempts. If consecutive unsuccessful log-on attempts exceed the established limit, a time delay before further log-on attempts are allowed shall disable the user account so it can only be reactivated by a system or security administrator.
- m. For systems that store, transmit, or process sensitive or confidential data, the agency shall password-protect the initialization (boot) settings.
- n. Account passwords shall not traverse the network or be stored in clear text. All passwords stored shall be encrypted.
- o. Passwords shall not be inserted into email messages or other forms of electronic

	Identification and Authentication Policy		
PR-AA-P3			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 5 of 9

communication without encryption.

- p. Passwords shall be different from all other accounts held by that user.
- q. Passwords shall not be revealed to anyone, including supervisors, help desk personnel, security administrators, family members, or co-workers.
- r. Users shall enter passwords manually for each application or system, except for simplified/single sign-on systems that have been approved by the State.
- s. Passwords shall be changed when suspicion or confirmation of system or password compromise occurs.
- t. End user identity shall be validated when a password reset is requested. Initial passwords and subsequent password resets shall use a unique password for each user account.

IA-5 (1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

Password-based authentication shall require:

- a. A regularly updated list of commonly used, expected, or compromised passwords to be reviewed at a State-defined frequency;
- b. Verification that passwords are not found on the list of commonly used, expected, or compromised passwords in point "a." above;
- c. Password transmission only over cryptographically protected channels;
- d. Storage of passwords using an approved salted key derivation function;
- e. Immediate selection of a new password upon account recovery;
- f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;
- g. Employ automated tools to assist users in selecting strong password authenticators; and
- h. Enforce the composition and complexity rules defined in IA-5.

IA-5 (2) AUTHENTICATOR MANAGEMENT | PUBLIC KEY-BASED AUTHENTICATION

All State information systems that require the use of a certificate for PKI authentication, including those operated on its behalf, shall ensure:



- a. The validation, protection, and mapping of that certificate;
- b. The certificate is valid (i.e., not expired, revoked, or marked invalid);
- c. Is associated with the corresponding user account that is attempting to authenticate;
- d. The certificate path is from an accepted trust point and that any intermediary trust points (sub certificate authorities) are valid;
- e. System stored private keys are protected; and
- f. System keys for contractor-based systems are controlled by a staff representative of the agency or OIT.

IA-5 (6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATION

Authenticators used to grant access to State systems shall be protected commensurate with the highest security category of information on those systems.

IA-6 AUTHENTICATION FEEDBACK

All State information systems, including those operated on its behalf, shall ensure that:

	Identification and Authentication Policy		
PR-AA-P3			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 6 of 9

- a. Authentication information feedback is obscured during the authentication process to protect the information from possible use by unauthorized individuals.
- b. Passwords are masked upon entry with asterisks or equivalent to prevent clear text display.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Mechanisms shall be implemented for authentication to a cryptographic module that meets the requirements of applicable federal and State laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.

All encrypted electronic transmissions must be encrypted using FIPS 140 validated cryptographic modules.

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Non-organizational users or processes acting on behalf of non-organizational users include system users other than organizational users explicitly covered by IA-2. For all State information systems accessible to the public (i.e., public-facing websites or portals), including those operated on behalf of the agencies, non-organizational users are uniquely identified and authenticated.

IA-8 (2) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF EXTERNAL CREDENTIALS

All State information systems accessible to the public, including those operated on behalf of the agencies, shall only approve third-party credentials that meet or exceed the set of minimum technical, security, privacy, and agency maturity requirements.

IA-8 (4) IDENTIFICATION AND AUTHENTICATION | USE OF DEFINED PROFILES

Unique identifiers for non-organizational users accessing information systems, including those operated on behalf of the agencies, shall conform to defined profiles as provided by OIT.

IA-11 RE-AUTHENTICATION

The State may require users to re-authenticate when:



- a. An account changes and necessitates re-authentication;
- b. A privileged function occurs;
- c. The user's role changes; or
- d. After a fixed period (e.g., 15 minutes).

IA-12 IDENTITY PROOFING

Organizations shall ensure user identity is established with evidence sufficient to resolve the user identity to a unique individual and collect, validate, and store supporting evidence.

IA-12 (2) IDENTITY PROOFING | IDENTITY EVIDENCE

Evidence of individual identification such as documentary evidence or a combination of documents and biometrics must be presented to the State registration authority owning identities validation and

	Identification and Authentication Policy		
PR-AA-P3			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 7 of 9

verification. This authority may use external sources/services for completion of the validation and verification of individual identities.

IA-12 (3) IDENTITY PROOFING | IDENTITY EVIDENCE VALIDATION/VERIFICATION

Identity evidence shall be validated and verified through State-defined documents and methods as listed below:

- a. ID card issued by federal, state, or local government;
- b. US Passport;
- c. Birth Certificate; and/or
- d. Permanent Resident Card.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

This is the first State of Alabama Identification and Authentication Policy. All State agencies and vendors of the State are required to comply with the current implemented version of this policy.



Identification and Authentication Policy



PR-AA-P3

Effective Date:
01/31/2025

Date Approved:
01/15/2025

Version:
1

Page #:
8 of 9

REVISION HISTORY

Revision Date	Summary of Change
12/31/2024	Policy Update

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK



Identification and Authentication Policy



PR-AA-P3

Effective Date:
01/31/2025

Date Approved:
01/15/2025

Version:
1

Page #:
9 of 9

APPROVED BY

Signature	<i>Daniel Urquhart</i>
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	01/15/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK