Division of Enterprise Technology Strategy and Services

ETSS Policy 300.7

Identification and Authentication Policy (IA)

Publish Date: 23 June 2026
Effective Date: 23 June 2026
Last Review: 22 June 2026

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes the requirements for identifying and authenticating user and device access to State of Rhode Island information systems and network resources. Identity is the primary pillar of the State's Zero Trust security architecture. This policy ensures that user access is authorized prior to system access, classified data is protected through strong authentication mechanisms, and accountability is maintained through unique identification and centralized identity services.

This policy supports the State's compliance with NIST SP 800-53 Revision 5 (Identification and Authentication family), NIST SP 800-63-3 (Digital Identity Guidelines), NIST Cybersecurity Framework 2.0, IRS Publication 1075, and other applicable federal and state regulatory requirements.

2. Applicability

This policy applies to all State of Rhode Island Executive Branch departments, including agencies, boards, and commissions, as well as their employees (permanent, non-permanent, full-time, and part-time), interns, consultants, contractors, vendors, and any entity that has access to State information systems and data, whether operated or maintained by the State or on behalf of the State.

3. Roles and Responsibilities

3.1. Chief Information Security Officer (CISO)

Designated as the official responsible for the enterprise Identification and Authentication policy. Approves exemptions from authentication requirements. Approves MFA token solutions and non-standard authentication mechanisms.

3.2. ETSS Identity and Access Management (IAM) Team

Responsible for managing enterprise identity services built on Active Directory and Microsoft Entra ID, enforcing MFA through enterprise Conditional Access policies, managing privileged access through CyberArk PAM, maintaining device authentication and compliance policies, and coordinating identity proofing with HR and agency onboarding processes.

3.3. Human Resources (HR)

Responsible for the initial identity proofing process through the Enterprise Resource

Planning (ERP) system, including verification of employment, contractual validation, and background attestation for new users prior to account provisioning.

3.4. System Owners

Responsible for ensuring identification and authentication controls are implemented for their systems, coordinating with ETSS IAM on system-specific authentication requirements, documenting authentication parameters in the System Security Plan, and requesting exemptions for legacy systems that cannot meet standard requirements.

3.5. Agency Technical Support Managers (TSMs)

Authorize physical authentication tokens for agency users, coordinate with ETSS Enterprise Security Team on MFA token approvals, manage agency-level identity management profiles for non-State employees, and support annual account recertification processes.

3.6. All Users

Responsible for maintaining the confidentiality of authenticators, completing MFA enrollment, re-authenticating when required, reporting compromised or lost authenticators immediately, and complying with all password and authentication requirements of this policy.

4. Procedures for Compliance

The following requirements establish the identification and authentication controls that agencies and ETSS must implement. Security controls are assigned based on the Information Assurance Level (IAL) of the information system, aligned to the NIST SP 800-53 Rev. 5 Moderate baseline.

4.1 Identification and Authentication Policy and Procedures (IA-1)

Applies to: All systems (IAL1, IAL2)

Each agency shall develop, document, and disseminate an identification and authentication policy and supporting procedures. The ETSS CISO is designated as the official responsible for the enterprise policy. The policy shall be reviewed at least every three (3) years and following significant changes. Supporting procedures shall be reviewed annually and updated following significant changes to systems, identity providers, authentication technologies, or regulatory requirements.

4.2 Identification and Authentication of Organizational Users (IA-2)

Applies to: All systems (IAL1, IAL2)

Information systems shall uniquely identify and authenticate system users or processes acting on behalf of users through enterprise identity services prior to granting system access. Each user shall be assigned a unique identifier consistently associated with all system actions and audit records. MFA is required for access to State enterprise systems and cloud services. Authentication events shall be centrally logged and monitored.

4.2.1 Multifactor Authentication to Privileged Accounts (IA-2(1))

Applies to: All systems (IAL1, IAL2)

Each agency shall implement MFA for all access to privileged accounts, including local, network, and remote access. Privileged access shall be centrally enforced through enterprise privileged access management (PAM) integrated with enterprise directory services. MFA shall include time-bound and approval-based privileged

access where applicable, with session monitoring, credential vaulting, and audit logging for all privileged actions.

4.2.2 Multifactor Authentication to Non-Privileged Accounts (IA-2(2))

Applies to: All systems (IAL1, IAL2)

Each agency shall implement MFA for access to non-privileged accounts, including all remote access connections. MFA enforcement for non-privileged accounts follows the same enterprise identity service integration as privileged accounts.

4.2.3 Individual Authentication with Group Authentication (IA-2(5))

Applies to: Moderate and above (IAL2)

When shared accounts or authenticators are employed, users shall be individually authenticated before granting access to shared accounts or resources. Group membership shall be used only to convey authorization and role context, not to replace individual identity. All authentication events shall remain uniquely attributable to an individual user identity.

4.2.4 Access to Accounts via Separate Device (IA-2(6))

Applies to: Moderate and above (IAL2)

Each agency shall implement MFA for local, network, and remote access to all accounts such that at least one authentication factor is provided by a device separate from the system being accessed (such as a hardware security key, mobile authenticator application, or certificate-based authenticator on a managed device). All MFA devices shall employ FIPS 140-2 or FIPS 140-3 validated cryptographic modules or equivalent mechanisms.

4.2.5 Replay-Resistant Authentication (IA-2(8))

Applies to: All systems (IAL1, IAL2)

Each agency shall implement replay-resistant authentication mechanisms for access to all accounts. Replay resistance shall be achieved through challenge-response methods, time-bound one-time authentication codes, certificate-based authentication with ephemeral session keys, and token-based authentication with short-lived access tokens.

4.3 Device Identification and Authentication (IA-3)

Applies to: Moderate and above (IAL2)

Each agency shall uniquely identify and authenticate end-user devices (workstations, laptops, VoIP phones, smartphones) via an appropriate method (such as certificate-based authentication, MAC address, RADIUS, Kerberos, TLS, or EAP) prior to establishing local, remote, or network connections. The agency shall maintain a list of approved devices or device types accepted for device identification and authentication.

4.4 Identifier Management (IA-4)

Applies to: All systems (IAL1, IAL2)

Each agency shall manage information system identifiers by:

a. Receiving authorization from designated personnel prior to assigning an identifier.

b. Selecting an identifier that uniquely identifies the individual, group, role, service, or device.

c. Assigning the identifier to the intended individual, group, role, service, or device.

d. Preventing reuse or reassignment of identifiers. Identifiers shall be disabled after no more than ninety (90) days of inactivity. Inactive accounts shall be revoked or deleted during the annual user account recertification process.

4.4.1 Identify User Status (IA-4(4))

Applies to: Moderate and above (IAL2)

Each agency shall manage and identify each non-State employee identifier as belonging to a contractor, vendor, or intern, enabling the enterprise to readily distinguish external users from State employees.

4.5 Authenticator Management (IA-5)

Applies to: All systems (IAL1, IAL2)

ETSS shall enforce compliance with authenticator requirements through implementation of appropriate technical controls (such as Active Directory Group Policy and Entra ID Conditional Access). If requirements cannot be enforced technically, the agency shall notify the ETSS CISO in writing prior to production deployment to obtain a formal exemption with compensating controls. Exemptions are valid for one (1) year and must be formally renewed. Each agency shall manage authenticators by:

a. Verifying the identity of the individual, group, role, service, or device receiving the authenticator. Users shall re-authenticate at each login and after each screen lock due to inactivity.

b. Establishing initial authenticator content and ensuring authenticators have sufficient strength for their intended use. Biometrics (fingerprint, facial recognition) are authorized as a second factor for device MFA.

c. Establishing procedures for initial distribution, lost/compromised/damaged authenticators, and revocation. Compromised accounts shall be disabled immediately.

d. Changing default authenticator content prior to first use.

e. Establishing authenticator lifetime restrictions and reuse conditions. Authenticators shall have a minimum lifetime of one (1) day and shall not be reused for a minimum of twenty-four (24) generations.

f. Protecting authenticators from unauthorized disclosure and modification. Users shall not share passwords. Shared account passwords requiring physical storage shall be secured in a sealed envelope within a locked container accessible only to authorized personnel.

g. Changing authenticators for group or role accounts upon a change in membership.

4.5.1 Password-Based Authentication (IA-5(1))

Applies to: All systems (IAL1, IAL2)

Each agency shall enforce the following password requirements:

a. Minimum length of fourteen (14) characters. Long passwords and passphrases are encouraged.

b. At least one character from at least three of the four categories: uppercase, lowercase, number, and non-alphanumeric special character.

c. Minimum lifetime of one (1) day; maximum lifetime of ninety (90) days for non-privileged accounts and sixty (60) days for privileged accounts.

d. Passwords shall not be identical to any of the previous twenty-four (24) passwords, shall not contain dictionary words, and shall not be identical to the user ID or email address.

e. Passwords shall be encrypted at rest (using an approved salted key derivation function) and during transmission (via encrypted channels only).

f. Users shall create a new password immediately after initial login and upon account recovery via the ETSS Enterprise Service Desk.

g. For devices using a PIN as the MFA authenticator, the PIN shall be a minimum of six (6) digits.

h. For legacy systems that cannot meet minimum complexity requirements, the strictest parameters the system allows shall be implemented and documented in the System Security Plan with an approved risk acceptance submission.

4.5.2 Public Key-Based Authentication (IA-5(2))

Applies to: Moderate and above (IAL2)

Each agency shall enforce authorized access to private keys, map authenticated identities to the corresponding account, and when PKI is utilized, validate certifications by constructing and verifying the certification path to an accepted trust anchor, including certificate status verification and a local cache of revocation data.

4.5.3 Protection of Authenticators (IA-5(6))

Applies to: Moderate and above (IAL2)

Each agency shall provide authenticators with protection commensurate with the highest security category of the information to which the authenticator permits access.

4.5.4 No Embedded Unencrypted Static Authenticators (IA-5(7))

Applies to: Moderate and above (IAL2)

Information systems and applications shall not embed unencrypted static authenticators (such as passwords, PINs, or cryptographic keys) in source code, scripts, configuration files, or other application artifacts. Embedded credentials shall be identified and migrated to enterprise secrets management or vault solutions.

4.6 Authentication Feedback (IA-6)

Applies to: All systems (IAL1, IAL2)

Information systems shall obscure authenticator information during the authentication process and shall not provide information that would allow the authentication mechanism to be compromised.

4.7 Cryptographic Module Authentication (IA-7)

Applies to: All systems (IAL1, IAL2)

Information systems shall implement authentication to cryptographic modules that meets FIPS 140-2 or FIPS 140-3 standards, as applicable.

4.8 Identification and Authentication of Non-Organizational Users (IA-8)

Applies to: All systems (IAL1, IAL2)

Information systems shall uniquely identify and authenticate non-organizational system users or processes acting on behalf of non-organizational users.

4.8.1 Acceptance of External Authenticators (IA-8(2))

Applies to: All systems (IAL1, IAL2)

Each agency shall accept only NIST SP 800-63B compliant external authenticators

for publicly accessible systems. MFA is required when PII is accessible via a public-facing system. A list of accepted external authenticators shall be documented and maintained.

4.8.2 Use of Defined Profiles (IA-8(4))

Applies to: All systems (IAL1, IAL2)

Each agency shall define identity management profiles to readily identify non-organizational users, including vendors, contractors, interns, temporary, and seasonal personnel.

4.9 Re-Authentication (IA-11)

Applies to: All systems (IAL1, IAL2)

Each agency shall require users to re-authenticate under the following circumstances: to release a session or screen lock due to inactivity, after an authenticator change, when the user's role changes (such as switching between standard and privileged accounts), when access transitions between trusted and untrusted networks, when device posture or compliance status changes, and when risk-based events or anomalous behavior are detected.

4.10 Identity Proofing (IA-12)

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Prior to granting logical access, collect, validate, and verify evidence that identifies the user based on appropriate identity assurance level requirements specified in ETSS and NIST SP 800-63-3 digital identity guidelines. Identity proofing shall be performed through the Enterprise Resource Planning (ERP) system, including HR onboarding, contractual validation, and background attestation. Users shall not be issued credentials until identity proofing is successfully completed. Physical authentication tokens used for MFA shall be authorized by the agency TSM and approved by the ETSS Enterprise Security Team.

b. Resolve user identities to a unique individual through employee ID and unique enterprise user account provisioning.

4.10.1 Identity Evidence (IA-12(2))

Applies to: Moderate and above (IAL2)

Each agency shall require that individual identification includes a government-issued photo document (such as a driver's license or passport) presented to the registration authority, with evidence consistent with the risk level of the associated systems, roles, and privileges.

4.10.2 Identity Evidence Validation and Verification (IA-12(3))

Applies to: Moderate and above (IAL2)

Each agency shall require that presented identity evidence is valid, current (not expired), and includes a photo that positively identifies the user.

4.10.3 Address Confirmation (IA-12(5))

Applies to: Moderate and above (IAL2)

Each agency shall require that a registration code or other identity proofing notice be delivered via an out-of-band method to verify the user's address of record.

5. Repercussions for Non-Compliance

Failure to comply with this policy may result in corrective action proportional to the severity of the violation. Consequences may include, but are not limited to:

a. Immediate revocation or suspension of system access for sharing credentials, bypassing MFA, or using unauthorized authentication methods.

b. Mandatory password reset and retraining on authenticator management requirements.

c. Formal counseling or written reprimand.

d. Referral to agency management for disciplinary proceedings, up to and including termination.

e. Denial of system authorization for systems that do not enforce enterprise identity and authentication requirements.

f. Agency financial responsibility for costs associated with mitigating unauthorized access resulting from non-compliance with this policy for which an exemption has not been granted.

Non-compliance findings shall be documented and tracked through ETSS governance processes and may be recorded in the agency Plan of Action and Milestones (POAM).

6. Approval / Review Signatures

Chief Information Security Officer (CISO)
Division of Enterprise Technology Strategy and Services (ETSS)

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services (ETSS)