# Identity and Authentication Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives.*

### **S**ecurity boundary under scope

1. [List of applicable systems]

### References

1. NIST 800-63: <https://pages.nist.gov/800-63-3/>
2. NIST 800-63B: <https://pages.nist.gov/800-63-3/sp800-63b.html>
3. ISO/IEC 29115: <https://www.iso.org/standard/45138.html>
4. ISO/IEC 24760: <https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:24760:-1:ed-2:v1:en>
5. ISO/IEC 27001:2022: A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.5
6. NIST 800-53 rev. 5: AC-1, AC-2, AC-2(1), AC-2(3), AC-2(7), AC-2(9), AC-3, AC-6(1), AC-6(2), AC-6(9), AC-7, AC-12, AC-17(4), CM-5(1), AU-9(4), IA-1, IA-2, IA-2(1), IA-2(2), IA-2(5), IA-2(6), IA-2(8), IA-3, IA-5, IA-5(1), IA-5, IA-5(6), IA-5(7), IA-6, IA-7, IA-8, IA-8(2), IA-8(4), IA-11, IA-12, IA-12(2), IA-12(3), SC-10
7. CIS v8: 3.3, 4.3, 4.7, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 6.1, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 12.5
8. PCI DSS 4.0: 7.1.1, 7.1.2, 7.2.1, 7.2.2, 7.2.3, 7.3.2, 8.1.1, 8.2.1, 8.2.2, 8.2.3, 8.2.6, 8.2.7, 8.2.8, 8.3.1, 8.3.2, 8.3.3, 8.3.4, 8.3.5, 8.3.6, 8.3.7, 8.3.8, 8.3.9, 8.3.10, 8.3.10.1, 8.3.11, 8.4.1, 8.4.2, 8.4.3, 8.5.1, 8.6.1, 8.6.2, 8.6.3
9. AICPA SOC 2 TSC: CC6.1, CC6.2, CC6.3, CC6.6, P5.1, P5.2

## Document ownership

 <(Choose from)>

* 1. Policy Owner:
		1. [Owner name] ([Owner email]), [Owner title]
	2. Information Security Officer:
		1. [Information officer name], ([Information officer email]), [Information officer title]
	3. System Owner(s):
		1. [System owner name], ([System owner email]), [System owner title]
	4. Process and Operational Owner(s)
		1. [process owner], ([process owner email]), [process owner title]
	5. System Administrator(s):
		1. [System admin name], ([System admin email]), [System admin title]
	6. Required Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT
	7. Optional Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT

## Purpose

The purpose of this Identity and Authentication Policy is to establish a framework for managing and authenticating user identities. This policy aims to ensure the security and integrity of the organization's data by implementing robust procedures for account creation, management, authentication, and access control. By adhering to these guidelines, the organization seeks to minimize the risk of unauthorized access, data breaches, and other security incidents.

## Scope

This policy applies to all employees, contractors, vendors, and other individuals or entities who have access to the organization's information systems. It encompasses all aspects of identity and authentication management, including but not limited to:

* Account creation and approval processes
* Ongoing account management and review
* Management of privileged accounts
* Procedures for account deactivation
* Re-authentication requirements
* Protection of authentication factors
* Implementation of multi-factor authentication (MFA)
* Password complexity standards
* Credential retry limits and account lockout mechanisms
* Prohibition of shared accounts
* Management of service accounts

The policy covers all information systems, applications, and services within the organization, including on-premises and cloud-based environments. Compliance with this policy is mandatory for all users and will be enforced by the Information Security Team in collaboration with system owners and administrators.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], **[owner title]** | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | **Executive Team** | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | **Executive Team** | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], **[Information officer title]** | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner], **Operational owner title]** |  |
| Information Systems Administrators | **System Administrators**  | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], **[HR title]** | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users |  **End Users** | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | **[provider type]** | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
	2. Management has reviewed and approved this policy.
	3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
	4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
	2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. **Account Creation**
		1. The process of establishing new user accounts, involving approval from appropriate authorities and the issuance of unique user IDs and passwords.
	2. **Account Management**
		1. The procedures and practices for managing user accounts, including defining account types, assigning account managers, authorizing access, and reviewing accounts for compliance.
	3. **Privileged Account Management**
		1. The oversight and administration of accounts with elevated privileges, ensuring appropriate role assignments, monitoring, revoking access, and implementing multifactor authentication.
	4. **Account Deactivation**
		1. The process of disabling user accounts when they are no longer needed, expired, inactive, or associated with a terminated employee, typically within a specified timeframe.
	5. **Re-authentication Events**
		1. The requirement for users to re-authenticate after a certain period of inactivity or continuous login to maintain security.
	6. **Protection of Authentication Factors**
		1. Measures to safeguard authenticators, such as passwords and tokens, to ensure they are not exposed or easily exploited.
	7. **Multi-Factor Authentication (MFA)**
		1. A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for access.
	8. **Password Complexity**
		1. The standards for creating strong passwords, including requirements for length, character types, and avoidance of common or compromised passwords.
	9. **Credential Retry and Lockout**
		1. Policies that limit the number of consecutive invalid login attempts and the automatic locking of accounts after exceeding this limit to prevent unauthorized access.
	10. **Prohibition of Shared Accounts**
		1. The policy that disallows the use of shared accounts unless explicitly justified and approved, ensuring individual authentication before access.
	11. **Service Accounts**
		1. Special user accounts used by applications or services to interact with the operating system, managed with the same rigor as user accounts, including creation, modification, and deactivation procedures.
	12. **System Owner**
		1. The individual responsible for the overall operation and maintenance of a system, including authorizing account creation and changes.
	13. **System Administrator**
		1. The individual responsible for maintaining the computer systems, including user account management and ensuring compliance with security policies.
	14. **Authenticator**
		1. A mechanism or token used to verify the identity of a user, such as passwords, biometric data, or security tokens.
	15. **Role-Based Access Scheme**
		1. An access control strategy where permissions are assigned based on the roles of individual users within an organization.
	16. **FIPS (Federal Information Processing Standards)**
		1. Standards for cryptographic modules that provide data encryption and other security measures, ensuring compliance with federal guidelines.
	17. **NSA-Approved Cryptography**
		1. Cryptographic algorithms and methods approved by the National Security Agency for use in securing sensitive information.
	18. **Inactive Account**
		1. An account that has not been used for a specified period, typically resulting in deactivation or additional verification requirements.
	19. **Emergency Accounts**
		1. Accounts created for temporary use during emergencies, with strict deactivation timelines to prevent misuse.
	20. **Temporary Accounts**
		1. Accounts created for short-term use, subject to deactivation within a predefined period or after a specific task is completed.

## Policy

#### Account Creation

The [responsible party] shall:

* + 1. Require approval from the System Owner for requests to create elevated privilege accounts such as System, Emergency, Developer, Administrator, Temporary, and Service accounts​​.
		2. Require System Administrators' approval for individual user accounts​​.
		3. Create and distribute unique user IDs and passwords for all users​​.
		4. Enforce a standardized naming convention for user IDs that indicates the responsible individual's name​​.

#### Account Management

The [responsible party] shall:

* + 1. Define and document the types of accounts allowed and specifically prohibited for use within the system​​.
		2. Assign account managers for information system accounts​​.
		3. Require System Owner approval for group and role membership​​.
		4. Authorize access to the information system based on a valid access authorization, intended system usage, and other attributes as required by organizational procedures​​.
		5. Review accounts for compliance with account management requirements at least every quarter​​.

#### Privileged Account Management

The [responsible party] shall:

* + 1. Establish and administer privileged user accounts in accordance with a role-based access scheme​​.
		2. Monitor privileged role or attribute assignments and changes​​.
		3. Revoke access when privileged role or attribute assignments are no longer appropriate​​.
		4. Implement multifactor authentication for network access to privileged accounts​​.

#### Account Deactivation

The [responsible party] shall:

* + 1. Disable user accounts within 24 hours when the accounts have expired, are no longer associated with a user or individual, are in violation of organizational policy, or have been inactive for 90 days​​.
		2. Immediately revoke all information systems access accounts upon an employee's termination​​.
		3. Align account management processes with personnel termination and transfer processes​​.

#### Re-authentication Events

The [responsible party] shall:

* + 1. Require users to re-authenticate when idle for 30 minutes and after 12 hours of continuous login​​.

#### Protection of Authentication Factors

The [responsible party] shall:

* + 1. Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access​​.
		2. Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage​​.
		3. Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation​​.

#### Multi-Factor Authentication (MFA)

The [responsible party] shall:

* + 1. Implement multi-factor authentication for network access to both privileged and non-privileged accounts​​.
		2. Ensure that one of the factors is provided by a device separate from the system gaining access, meeting FIPS validated or NSA-approved cryptography​​.

#### Password Complexity

The [responsible party] shall:

* + 1. Enforce the following password composition and complexity rules:
			1. Passwords must contain both upper- and lower-case characters.
			2. Passwords must include digits and punctuation characters as well as letters.
			3. Passwords must be at least 14 alphanumeric characters long​​.
		2. Verify, when users create or update passwords, that the passwords are not found on a list of commonly used, expected, or compromised passwords​​.

#### Credential Retry and Lockout

The [responsible party] shall:

* + 1. Enforce a limit of no more than three consecutive invalid logon attempts by a user during a 15-minute time period​​.
		2. Automatically lock the account/node for 30 minutes or until released by an administrator when the maximum number of unsuccessful attempts is exceeded​​.

#### Prohibition of Shared Accounts

The [responsible party] shall:

* + 1. Prohibit the use of shared accounts unless a business case, justification statement, and approval from the System Owner and the Information Security Team are provided​​.
		2. Ensure users are individually authenticated before granting access to shared accounts or resources​​.

#### Service Accounts

The [responsible party] shall:

* + 1. Manage service accounts with the same level of rigor as user accounts​​.
		2. Ensure that service accounts are created, enabled, modified, disabled, and removed in accordance with approved procedures​​.
		3. Disable temporary and emergency accounts no more than 96 hours after last use​​.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
	2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
	3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
		1. Policies
		2. Procedures
		3. Standards
		4. Documentation
		5. Regulations
		6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
	2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
		1. The Information Security Officer
		2. Officer of the [Organization name] Leadership Team
	3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |