

Password and Authentication Policy

Purpose

Authentication is the control that binds an identity to every action taken on Your Organization systems. Weak authentication undermines every downstream control — access control, logging, data protection, and incident response. This policy establishes Your Organization's minimum requirements for passwords, multi-factor authentication (MFA), and credential management across human and non-human identities.

Scope

This policy applies to all authentication to Your Organization information systems — corporate identity provider, SaaS applications, internal systems, databases, infrastructure consoles, VPN and zero-trust gateways, physical access systems, and service accounts. It applies to all workforce members, contractors, and third parties.

Password requirements

Your Organization follows the modern guidance in NIST SP 800-63B: long, uncommon passwords are stronger than short, frequently rotated, complex ones.

- **Length.** Minimum 14 characters for interactive user accounts. Minimum 20 characters for privileged accounts and service accounts.
- **Composition.** No mandatory complexity classes. Users are required to choose passwords that are not found in common-password blocklists.
- **Blocklist screening.** New and changed passwords are screened against a dictionary of known-compromised credentials; matches are rejected.
- **Reuse.** Passwords must be unique to Your Organization. Reuse of a password from any other system is prohibited.
- **Rotation.** Interactive user passwords do not require periodic rotation absent evidence of compromise. Privileged and service-account credentials are rotated at least annually and immediately on a leaver event.
- **Storage on the server side.** Passwords are never stored in cleartext or with reversible encryption. Your Organization uses salted, modern, memory-hard hashing (Argon2id, scrypt, or equivalent) wherever it controls the hash.
- **Storage on the user side.** Workforce members must use the Your Organization-approved password manager and must not reuse, write down, or email passwords.

Multi-factor authentication

MFA is **required** on:

- The corporate identity provider and every federated SaaS application.

- VPN and zero-trust gateways.
- Privileged consoles (cloud root/admin, production databases, deployment systems, secrets management).
- Any authentication to systems handling Restricted data.

Accepted factors, in order of preference:

1. Phishing-resistant (FIDO2 security keys, platform authenticators with WebAuthn).
2. Authenticator-app one-time codes (TOTP) or push notifications with number matching.
3. SMS one-time codes — permitted only as a temporary fallback for a named list of systems; deprecated and not accepted on privileged systems.

Service accounts and non-human identities

Non-human identities must authenticate with long secrets or short-lived credentials:

- API keys, OAuth client secrets, and SSH keys are a minimum of 20 characters or equivalent entropy.
- Where the platform supports it, use short-lived, workload-federated credentials (OIDC, cloud IAM roles) instead of static keys.
- Every non-human credential has a named human owner, a documented purpose, and a scheduled rotation.
- Non-human credentials are stored only in an approved secrets manager — never in source code, tickets, chat, or unencrypted configuration files.

Session management

- Session lifetime for interactive users is capped at 12 hours, with idle re-authentication after one hour on privileged systems.
- Authentication cookies are Secure, HttpOnly, and SameSite where the platform allows.
- On logout, sign-out, or password reset, active sessions for that identity are invalidated.

Lost, compromised, or suspected-compromised credentials

Users must report suspected credential compromise immediately to the security team. The security team rotates or revokes affected credentials, invalidates sessions, and investigates for signs of abuse.

Scope exceptions

Legacy systems that cannot meet these requirements must be documented on the exception register with compensating controls (e.g. network isolation, additional logging) and a remediation plan. Exceptions are approved by the CISO or designee and are time-bound.

Review cadence

This policy is reviewed annually by the Information Security team, or sooner if NIST guidance, regulatory requirements, or Your Organization's authentication tooling change materially.

Effective date: [the date this policy takes effect]