

Password Policy Template

A free, adaptable template covering password creation, MFA, storage, and enforcement requirements, aligned to current NIST guidance and mapped to SOC 2 / ISO 27001 / HIPAA / PCI DSS / GDPR.

Company: _____

Effective date: _____

Policy owner: _____

Review cycle: Annually, and after any NIST guidance update

HOW TO USE THIS TEMPLATE

Replace every bracketed placeholder with your organization's specifics, route the completed policy through your normal internal-approval process, and configure your identity provider to technically enforce the settings below before treating this as adopted. This template is a starting point, not legal advice — see ComplyJet's full Password Policy Template guide for the reasoning behind each section.

1. Purpose and Scope

This policy defines how [Company Name] creates, stores, changes, and enforces passwords across all systems the company controls. It establishes minimum requirements so that any employee, contractor, or auditor can determine what is expected without a case-by-case judgment call.

This policy applies to all employees, contractors, and service accounts, across all systems that require authentication, including production, staging, and development environments, and any system managed on the company's behalf by a third-party vendor.

2. Password Creation Requirements

Passwords must meet the following minimums, based on NIST SP 800-63B-4 (2025):

- **Minimum length:** 15 characters when used as the sole authentication factor, or 8 characters when combined with an approved multi-factor authentication method.
- **No forced composition rules.** Mandatory special characters or mixed case are not required.
- **No mandatory periodic rotation.** Passwords are changed only on evidence of compromise or a role/access change, not on a fixed calendar.
- **Mandatory breach screening.** New passwords are checked against known-breached and commonly-used password lists at the time of creation; any match is rejected.
- **No reuse across systems.** A password used for one company system may not be reused for another.

SAMPLE CLAUSE — PASSWORD CREATION REQUIREMENTS

All passwords must be a minimum of 15 characters when used as the sole authentication factor, or a minimum of 8 characters when combined with an approved multi-factor authentication method. Mandatory complexity rules (special characters, mixed case) are not required. New passwords are screened against a list of known-breached and commonly-used passwords at the time of creation; any match is rejected. Passwords may not be reused across company systems.

3. Multi-Factor Authentication Requirements

Multi-factor authentication (MFA) is a required companion control, not optional hardening. Name exactly which systems require it rather than "where possible."

- MFA is required for [all systems handling customer data, production infrastructure, email, and the identity provider itself — list explicitly].
- Phishing-resistant methods (hardware security keys, passkeys) are preferred over SMS-based codes.
- MFA is enabled at account creation, not left as an optional setting the user can decline.

4. Password Storage and Manager Requirements

A strong password requirement is only as good as how it is stored. This section closes the gap between a strong password policy and weak practice.

- An approved password manager is mandatory for all company-related credentials.
- Browser-saved passwords and written-down (physical or plaintext digital) passwords are explicitly prohibited.
- Shared credentials must be stored and shared only through the approved password manager's sharing feature, never over email, chat, or a shared document.

5. Account Lockout and Monitoring

Account lockout settings show that the policy is technically enforced, not just written.

- Accounts lock after [5] consecutive failed login attempts within [15] minutes.
- A locked account requires [IT/Security team] intervention or an approved self-service unlock flow to restore access.
- Repeated failed-login patterns are monitored and flagged for review, not just silently logged.

6. Exceptions Process

Any exception to this policy, such as a legacy system that cannot technically support current requirements, requires documented approval from [Policy Owner / Security Lead] and a compensating control, logged in [exceptions register / ticketing system]. Exceptions are reviewed at the same cadence as this policy and re-justified or remediated, not renewed indefinitely by default.

7. Enforcement and Ownership

[Policy Owner] is accountable for this policy's accuracy, enforcement, and review. Enforcement is primarily technical, through identity provider (SSO) configuration, not individual memory or discretion.

SAMPLE CLAUSE — ENFORCEMENT

This policy is enforced primarily through identity provider (SSO) configuration, not individual memory or discretion. The IT/Security lead configures minimum-length and MFA requirements to match this document, monitors failed-login thresholds, and reviews logged exceptions quarterly. Any system that cannot technically enforce these settings must be recorded under the Exceptions process.

8. Review Cadence

This policy is reviewed at least annually, and immediately following any material change to NIST guidance, a relevant compliance framework, or the company's identity-provider configuration.

9. Framework Alignment

How this policy's requirements map to the compliance frameworks most companies encounter. This is a starting reference, not a substitute for reading each framework's current text.

Framework	Where It Lives	What It Requires
SOC 2	Trust Services Criteria CC6.1–CC6.3	No fixed numeric rules; expects authentication strength, provisioning/offboarding, and periodic access review justified against a recognized standard.
ISO 27001	Annex A control 5.17, Authentication Information	Requires a formal process for allocating and managing authentication information; no mandated length, but expects a documented, enforced policy.
HIPAA	Security Rule, 45 CFR §164.312(a) / (d)	Requires access-control and identity-verification procedures; technology-neutral, sets no specific length, complexity, or rotation parameters.
PCI DSS 4.0	Requirement 8.3, Strong Authentication	Most prescriptive: 8.3.6 sets a 12-character minimum (8 if unsupported); 8.3.9 requires 90-day rotation for password-only auth, unless risk is analyzed dynamically.
GDPR	Article 32, Security of Processing	Requires "appropriate technical and organisational measures"; a documented password policy is commonly cited as evidence of meeting this requirement.

10. Roles and Responsibilities

Role	Responsibility
[Policy Owner]	Accountable for this policy's accuracy, enforcement, and annual review.
IT / Identity team	Configures identity-provider settings to technically match this policy's minimums; manages account lockouts.

Role	Responsibility
Security / Compliance team	Audits actual enforcement against this policy; manages the exceptions process.
All employees and contractors	Use the approved password manager and enrolled MFA method for every company system.

11. Rollout and Policy Maintenance

- 1 **Assign an owner** — usually the IT or security lead, accountable for the policy and its enforcement.
- 2 **Get leadership to formally approve it**, so it's an adopted policy, not a draft.
- 3 **Communicate it during onboarding**, not as a standalone memo employees never open.
- 4 **Configure identity-provider settings** so the written minimums are technically enforced, not just described.
- 5 **Require the approved password manager** as part of account setup, not an optional recommendation.
- 6 **Set a review date on the calendar**, so the policy doesn't quietly go stale as guidance changes.

BEFORE CALLING ROLLOUT COMPLETE

Confirm your identity provider's actual configuration (minimum length, MFA enforcement, lockout threshold) matches every number written in Sections 2–5. A policy that hasn't been checked against the live configuration isn't rolled out — it's just written.

Produced by ComplyJet as a free companion to the Password Policy Template: What to Include guide. ComplyJet helps SaaS startups turn policies like this one into evidence-backed controls across SOC 1, SOC 2, ISO 27001, HIPAA, GDPR, PCI DSS, and 25+ other frameworks. Book a free demo to see how.