LastPass

Password Policy Template

A starting framework for your organization. Adapt each section based on your compliance requirements, risk profile, and tooling.

Section 1: Scope

Define who this policy applies to: all employees, contractors, vendors with system access, and any third parties with credentials to company systems.

Section 2: Password Creation Requirements

- Minimum 14 characters for standard accounts
- Minimum 16 characters for admin and privileged accounts
- Maximum of at least 64 characters
- Permit all ASCII and Unicode characters, including spaces
- No mandatory composition rules
  (e.g., must include one uppercase, one special character)
- Where supported by your tooling, screen new passwords against known breach databases and common password dictionaries
- Passwords must not include the company name, the user's username, or sequential/ repeated characters

Section 3: Account Protection

- MFA required for all users (authenticator app preferred over SMS)
- Accounts locked after 5-8 failed login attempts
- Lockout duration of 30+ minutes or until admin intervention
- Session timeout after 15 minutes of inactivity for sensitive systems

Section 4: Password Handling and Storage

- Passwords must never be shared via email, Slack, or other unencrypted channels
- All credentials must be stored in an approved password manager
- Credentials saved in browsers must be migrated to the company vault
- Shared credentials must be distributed through the password manager's secure sharing features, with access revoked when no longer needed

Section 5: Change and Expiration

- No mandatory periodic changes for standard accounts
- Immediate change required if:
  - The credential appears in a known breach
  - The account shows signs of unauthorized access
  - The employee leaves the organization or changes roles
- For environments subject to PCI DSS: credentials for in-scope systems must be changed every 90 days

Section 6: Role-Based Requirements

Define at least two tiers:

	Standard Users	Privileged / Admin Accounts
Password minimum	14+ characters	16+ characters
MFA	Required	Required
Session Timeout	Standard	Shorter (e.g., 10 min)
Offline access	Permitted	Blocked
Additional logging	Standard	Required

Section 7: Enforcement and Monitoring

- Specify which tools enforce the policy (password manager, identity provider, GPOs)
- Define who is responsible for monitoring compliance (IT admin, security team, etc.)
- Document how violations are detected (security dashboards, breach monitoring, SaaS visibility tools)
- Describe how violations are remediated (forced reset, notification, account lockout)
- Set a review cadence: annually at minimum, or after any significant security event

---

This template is a starting point. Customize each section to reflect your organization's compliance requirements (HIPAA, PCI DSS, SOC 2, etc.), risk profile, and the specific tools you use to enforce your policy.