FREE RESOURCE / XBITIUM SECURITY

Password Policy Template

Aligned with current NIST guidance — not the outdated rules everyone copies.

Copy this into your own document, fill in the bracketed fields, and adopt it. It reflects **current** NIST SP 800-63B guidance, which reversed years of counterproductive advice. If your existing policy forces a password change every 90 days and demands a symbol, a number, and a capital letter, it is quietly teaching your staff to write passwords on sticky notes. This one does the opposite.

WHAT CHANGED, AND WHY

Forced rotation and complexity rules were shown to make passwords *weaker* — people simply append a '1' or a '!' in predictable ways. Modern guidance favours length, blocking known-breached passwords, and multi-factor authentication. Length beats complexity; a passphrase beats a scramble.

1. Purpose and scope

This policy defines how staff at **[Company name]** create and protect the passwords used to access company systems, email, and data. It applies to all employees, contractors, and anyone with access to company accounts.

2. Password requirements

- **Minimum length of 12 characters.** Longer is stronger. A passphrase of four random words is both easier to remember and harder to crack than a short scramble.
- **No mandatory complexity rules.** We do not require a specific mix of symbols and cases. Length and uniqueness matter more.
- **Every password must be unique.** A password reused from any other site is considered already compromised.
- **Passwords are screened against known breach lists.** Any password found in a public breach must be changed immediately.
- **No routine forced expiry.** Passwords are changed when there is reason to believe they may be compromised — not on an arbitrary calendar.

3. Multi-factor authentication (MFA)

MFA is **mandatory** for email, VPN, remote access, financial systems, and any administrator account. Where possible use an authenticator app or hardware key rather than SMS codes. MFA is the single most effective control against stolen passwords — a leaked password is far less dangerous when a second factor is required.

4. Password managers

Staff are **required** to use the company-approved password manager: **[e.g. 1Password / Bitwarden]**. Passwords must never be stored in spreadsheets, documents, browsers on shared machines, sticky notes, or plain-text files. Nobody can remember dozens of strong, unique passwords; the tool exists so they do not have to.

5. Protecting credentials

- Never share your password with anyone, including IT or management.
- Never enter your password after clicking a link in an email — navigate to the site directly. This is exactly how credential phishing works.
- Report any suspected password compromise immediately to **[contact]**. You will never be penalised for reporting quickly.
- Service and shared accounts must have a named owner and be documented.

6. Administrator and privileged accounts

- Admin accounts must use a different, unique password from the same person's everyday account.
- Admin rights are granted only to those who genuinely require them for their role.
- Privileged access is reviewed at least **[quarterly]** and removed promptly when no longer needed.

7. When someone leaves

Access for departing staff and ended contracts is revoked on the **same day** the relationship ends. Shared passwords those individuals knew are rotated. Ex-user accounts are a common and low-effort way for attackers to get back in.

8. Enforcement

Compliance is a condition of system access. Deliberate or repeated violations may result in disciplinary action. The goal, however, is protection — not punishment. Staff who report mistakes quickly help protect everyone.

Policy owner	*[Name / role responsible for this policy]*
Approved by	*[Name, title]*
Effective date	*[Date]*
Review date	*[Recommended: review annually]*

This resource is provided free of charge by Xbitium Technologies LLC as general guidance. It is not legal advice and does not create a professional relationship. Regulated organizations should confirm requirements with qualified counsel or a compliance professional. Regulated industries (healthcare, finance, government contractors) may have specific password requirements that exceed this baseline.