halved

Password Policy

v1.0 · Reviewed Jun 2026 · Next review Jun 2027

HALVED LIMITED

PASSWORD POLICY

Version: 1.0 Effective Date: 4th June 2026 Last Review: 4th June 2026 Next Review: 4th June 2027

Owner: Andrew James, CEO

1. PURPOSE

This policy defines password requirements for all Halved Limited systems to protect against unauthorised access and meet Cyber Essentials requirements.

2. SCOPE

This policy applies to all passwords used to access:

- Halved email accounts (Microsoft 365)
- Cloud services (Azure, GitHub, MongoDB Atlas, Cloudflare, Xero, etc.)
- macOS user accounts
- Any other systems containing organisational data

3. PASSWORD REQUIREMENTS

3.1 Minimum Password Standards

All passwords must meet the following minimum requirements:

- Minimum length: 10 characters
- No maximum length restriction

- Complexity: Use a passphrase (three or more random words) OR a mix of upper/lowercase letters, numbers, and symbols
- Uniqueness: Each system must have a unique password - never reuse passwords across services

3.2 Multi-Factor Authentication (MFA)

- MFA is required on all systems that offer it
- **Preferred MFA method:** Authenticator app (Microsoft Authenticator, Google Authenticator, or similar)
- **Acceptable MFA method:** SMS codes (where authenticator app is not available)
- **Not acceptable:** Email-based MFA does not count as true MFA

3.3 Password Management Requirement

All users must:

- Use a password manager to store passwords securely
- **Recommended password managers:** 1Password, Bitwarden, or macOS Keychain
- Never store passwords in plain text (documents, spreadsheets, notes apps)
- Never share passwords via email, Slack, or messaging

3.4 Admin Account Passwords

Administrative accounts require additional security:

Minimum length: 12 characters (must be different from standard account passwords)

MFA: Mandatory on all admin accounts

Uniqueness: Admin account passwords must be completely different from standard account passwords

4. PASSWORD CREATION GUIDANCE

4.1 Creating Strong Passwords

Good approaches:

- **Three random words:** CorrectHorseBatteryStaple
- **Passphrases:** ILove2DrinkCoffeeInTheMorning!
- **Password manager generated:** Let your password manager create a random strong password

Avoid:

- **Common patterns:** Password123, CompanyName2026
- **Personal information:** birthdays, names, addresses
- **Keyboard patterns:** qwerty123, asdfgh
- **Dictionary words on their own:** elephant (too weak without additional characters)

4.2 Password Expiry

- No forced password changes: Passwords do not expire on a schedule
- Change immediately if: You suspect your password has been compromised
- Change immediately if: A service reports a breach

5. COMPROMISED PASSWORDS

If you suspect your password has been compromised:

- Report immediately: Notify the CEO (Andrew James) within 1 hour
- Change the password immediately on the affected account
- Check for reuse: If you reused the password elsewhere, change it on all systems
- Re-enrol MFA if MFA may have been compromised
- Monitor account activity for unusual behaviour

6. NEW USER ONBOARDING

When a new team member joins:

- They are provided with this Password Policy during onboarding

- They set up a password manager before accessing any Halved systems
- They enable MFA on all accounts during first login
- CEO verifies MFA is enabled before granting access to sensitive systems

7. COMPLIANCE

Failure to comply with this policy may result in:

- Account suspension
- Disciplinary action
- Cyber Essentials certification failure

8. TRAINING

All users receive password security training:

- During onboarding (new users)
- Annually (refresher for existing users)
- After any security incident

APPROVED BY:

Andrew James, CEO Halved Limited Date: 4th June 2026

Questions about data protection? **dataprivacy@halved.io**

Website **halved.io** · students log in at my.halved.io

Halved Limited · registered in England and Wales, company number 15261677 · last updated June 2026