Password & Access Control Policy

For Australian Small & Medium Enterprises

Template Version 1.0 | December 2024

Important Notice

This template provides general guidance on password and access control. Specific requirements should be tailored to your organisation's systems and risk profile. Consider industry standards and security frameworks when implementing.

1. Purpose

This policy establishes requirements for password management and access control at [Company Name]. Strong passwords and proper access controls are essential to protect company systems, data and resources from unauthorised access.

2. Scope

This policy applies to:

- All employees, contractors and authorised users
- All systems, applications and accounts
- Both company-provided and personal devices used for work
- All forms of authentication credentials

3. Password Requirements

3.1 Password Complexity

All passwords must meet the following minimum requirements:

- Minimum length: 12 characters (or as enforced by system)
- Must contain at least one uppercase letter
- Must contain at least one lowercase letter
- Must contain at least one number
- Must contain at least one special character (!@#$%^&*)
- Must not be a dictionary word or common phrase

3.2 Password Creation Guidelines

When creating passwords:

- Use passphrases where possible (e.g., "Coffee4Morning!Walk")

- Do not use personal information (names, birthdays, etc.)
- Do not use sequences (123456, abcdef)
- Do not use keyboard patterns (qwerty, asdfgh)
- Each account should have a unique password

3.3 Password Changes

- Passwords must be changed every [90 days / as required by system]
- New passwords must not match any of the last [5] passwords
- Passwords must be changed immediately if compromise is suspected
- Temporary passwords must be changed on first login

4. Password Protection

4.1 Keeping Passwords Secure

- Never share passwords with anyone, including IT staff
- Do not write passwords on paper or sticky notes
- Do not store passwords in unencrypted files
- Do not send passwords via email or messaging
- Do not use the same password for work and personal accounts

4.2 Password Managers

[Company Name] [recommends/requires] the use of approved password managers:

- Use company-approved password manager solutions
- The master password must be strong and memorable
- Enable additional security features (2FA) on password managers
- Do not store the master password anywhere

5. Multi-Factor Authentication (MFA)

5.1 MFA Requirements

Multi-factor authentication is required for:

- All remote access to company systems
- Access to sensitive systems and data
- Email and collaboration platforms
- Administrative accounts
- Financial systems

5.2 Approved MFA Methods

- Authenticator apps (preferred)
- Hardware security keys

- SMS codes (where other methods unavailable)
- Biometric authentication on approved devices

5.3 MFA Best Practices

- Never share MFA codes with others
- Report lost or stolen MFA devices immediately
- Do not approve MFA prompts you did not initiate
- Keep backup codes secure

6. Access Control Principles

6.1 Least Privilege

- Access is granted based on job requirements
- Users receive minimum necessary access
- Access is not granted "just in case"
- Elevated access is temporary and task-specific

6.2 Need to Know

- Access to sensitive information is restricted
- Access requests must be justified
- Managers approve access for their team members

7. User Account Management

7.1 Account Creation

- Accounts created through formal request process
- Unique user ID for each person
- No shared accounts except where technically required
- Access set according to role requirements

7.2 Account Maintenance

- Regular review of account access
- Update access when roles change
- Remove access no longer needed
- Document all access changes

7.3 Account Termination

- Accounts disabled immediately when employment ends
- Access removed when no longer required
- Accounts deleted after appropriate retention period

8. Privileged Access

8.1 Administrative Accounts

- Separate accounts for administrative functions
- Administrative access limited to those who need it
- Enhanced monitoring of privileged accounts
- Regular review of administrative access

8.2 Service Accounts

- Unique service accounts for applications
- Strong passwords for service accounts
- Regular password rotation
- Access limited to required functions

9. Account Lockout

[Company Name] implements account lockout to prevent brute force attacks:

- Accounts lock after [5] failed login attempts
- Lockout duration: [30 minutes / until reset]
- Contact IT/Help Desk to unlock accounts
- Repeated lockouts will be investigated

10. Session Management

- Automatic session timeout after [15 minutes] of inactivity
- Log out when leaving workstation unattended
- Do not leave sessions logged in overnight
- Close browser sessions to sensitive applications

11. Remote Access

When accessing systems remotely:

- Use approved VPN connections
- MFA is required for all remote access
- Do not use public computers for sensitive access
- Ensure physical privacy when entering credentials
- Log out completely when finished

12. Reporting Security Incidents

Report immediately to IT/Security:

- Suspected password compromise

- Suspicious login attempts
- Unexpected MFA prompts
- Lost or stolen devices
- Phishing attempts
- Unauthorised access attempts

13. Access Reviews

[Company Name] conducts regular access reviews:

- Quarterly review of privileged access
- Annual review of all user access
- Review after role changes
- Remove unnecessary access promptly

14. Responsibilities

14.1 Users

- Create and maintain strong passwords
- Protect credentials from disclosure
- Use MFA where required
- Report security concerns
- Log out when finished

14.2 IT/Security

- Implement password policies
- Manage access control systems
- Conduct access reviews
- Respond to security incidents

14.3 Managers

- Approve appropriate access for team
- Notify IT of role changes
- Participate in access reviews

15. Policy Breaches

Breaches of this policy may result in:

- Immediate account suspension
- Disciplinary action
- Termination of employment for serious breaches

- Legal action where appropriate

16. Review

This policy will be reviewed:

- At least annually
- When security threats change
- When technology changes
- After security incidents

Employee Acknowledgement

I acknowledge that I have read and understood [Company Name]'s Password & Access Control Policy. I understand my responsibilities for protecting access credentials and agree to comply with this policy.

Employee Name: _____

Signature: _____

Date: _____