I.T Password Policy

AWAKEN ENERGY

The purpose of this Password Policy is to establish guidelines for creating, managing, and securing passwords used to access Awaken Energy's information systems. This policy ensures protection against unauthorised access and aligns with security best practices.

This policy applies to all employees, contractors, and third-party service providers who access Awaken Energy's:

- IT infrastructure and network systems
- Business applications, including Salesforce and AWS
- API integrations
- Email, cloud storage, and third-party software

Password Requirements

- Must be at least **12 characters long**.
- Must include at least **one uppercase letter, one lowercase letter, one number, and one special character**.
- Cannot be **reused** from the last **five passwords**.
- Must be changed **every 90 days**.
- Must not be **shared** or **written down** in unsecured locations.

Multi-Factor Authentication (MFA)

- Multi-Factor Authentication (MFA) is required for accessing critical systems, including Salesforce, AWS, and administrative accounts.
- SMS-based authentication is discouraged; authentication apps (e.g., Google Authenticator, Microsoft Authenticator) are preferred.

Password Storage & Management

- Employees must use **company-approved password managers** to store credentials securely.
- Passwords must never be stored in plaintext or shared via email or messaging applications.

Account Lockout & Failed Login Attempts

- Accounts will be locked **after five failed login attempts**.
- Locked accounts can only be reset by authorised IT personnel.
- Users must verify their identity before password resets.

Default & Temporary Passwords

- Default passwords must be **changed immediately** upon first login.
- Temporary passwords must expire within **24 hours**.
- Temporary passwords must follow the same complexity requirements as standard passwords.

Remote Access Security

- Remote access to company systems requires the use of **MFA**.
- Employees must log out of systems when not in use.
- Personal devices used for work must comply with security policies and have up-to-date security software.

Compliance & Enforcement

- Any violation of this policy may result in **disciplinary action**.
- IT security audits will be conducted to ensure compliance.
- This policy aligns with industry best practices and regulatory standards, including the **Australian Privacy Principles (APPs)**.