Cyber Security Policy

AWAKEN ENERGY

At Awaken Energy, we are committed to protecting the confidentiality, integrity, and availability of our information assets. This policy outlines the cyber security measures required to safeguard our systems, data, and customer information from threats, breaches, and unauthorised access.

This policy applies to all employees, contractors, vendors, and stakeholders who have access to Awaken Energy's IT systems, networks, and data. It covers all devices, applications, and digital communication methods used for business operations.

Responsibilities

Management Responsibilities:

- Implement and enforce cyber security policies and best practices.
- Provide training and resources to employees on cyber security awareness.
- Monitor and update security measures regularly.
- Investigate and address security breaches promptly.

Employee Responsibilities:

- Follow all cyber security guidelines and report suspicious activities.
- Use strong passwords and multi-factor authentication (MFA) where applicable.
- Ensure work devices are secure and up to date.
- Avoid accessing company data on unsecured public networks.
- Do not share confidential information without proper authorisation.

Cyber Security Best Practices

Access Control:

- Restrict access to sensitive data based on job roles.
- Use secure login credentials and enable MFA for critical systems.
- Lock devices when unattended and log out of systems when not in use.

Data Protection:

- Store and process personal and customer data in compliance with the Australian Privacy Act 1988.
- Encrypt sensitive information in storage and during transmission.
- Back up critical data regularly and store backups securely.

Device and Network Security:

- Install and maintain up-to-date anti-virus and security software.
- Secure Wi-Fi connections and avoid using untrusted networks.
- Prohibit the use of personal USBs or external storage devices on company computers without approval.

Email and Internet Use:

- Be cautious of phishing emails and suspicious links.
- Do not download or open attachments from unknown sources.
- Avoid accessing non-business-related or malicious websites on work devices.

Incident Reporting and Response:

- Report any suspected data breaches, security threats, or cyber attacks immediately to the IT security team.
- Follow the established incident response plan in case of a breach.
- Cooperate with investigations and remediation efforts.

Compliance with Australian Laws and Regulations

This policy aligns with the following Australian cyber security laws and guidelines:

- **Privacy Act 1988 (Cth) and Australian Privacy Principles (APPs)**
- **Notifiable Data Breaches (NDB) scheme**
- **Australian Signals Directorate (ASD) Essential Eight Mitigation Strategies**
- **Cyber Security Strategy 2020 and relevant industry standards**

Training and Awareness

- Employees must complete cyber security awareness training during onboarding and at regular intervals.
- Regular updates and refresher courses will be provided to ensure compliance with evolving threats and best practices.