Awaken Energy Physical Security Policy

This Physical Security Policy establishes the security measures and procedures required to protect Awaken Energy's assets, facilities, personnel, and any sensitive data, from unauthorised access, theft, damage, or loss.

This policy applies to all Awaken Energy employees, contractors, visitors, and any individuals who access company premises, equipment, or systems.

Access Control

- Only authorised personnel are permitted to enter restricted areas where sensitive business operations or data handling occur.
- All employees must use their company-issued ID badges for access to secure areas.
- Visitors must be pre-approved, logged upon arrival, and escorted at all times while in restricted zones.
- Remote access to IT infrastructure is restricted to authorised users with multi-factor authentication (MFA).

Facility Security

- All office premises and workspaces must remain locked outside of business hours.
- Security cameras (if applicable) monitor key access points and restricted areas.
- Physical keys, access cards, or biometric security measures are used to control entry.
- Fire alarms and emergency response protocols must be maintained in accordance with safety regulations.

Device Security & Asset Management

- Laptops, workstations, and any mobile devices used for company operations must be password-protected and encrypted.
- Automatic screen lock must be enabled on all company devices after a period of inactivity.
- All removable media (e.g., USB drives) are prohibited unless explicitly approved for business purposes and must be encrypted.
- Devices must be stored in secure locations when not in use and transported securely when taken offsite.

Cloud & Data Centre Security

- Awaken Energy utilises cloud-based platforms (Salesforce and AWS) with security controls inherited from ISO 27001 and SOC 2 Type 2-certified environments.
- Physical access to data centres is strictly managed by AWS and Salesforce with 24/7 surveillance and biometric access controls.
- Employees do not have direct physical access to cloud data centre infrastructure.

Secure Disposal of Assets & Sensitive Materials

- Electronic devices containing sensitive data must be securely wiped using NIST 800-88-compliant methods before disposal.
- Devices that cannot be securely wiped must be physically destroyed or disposed of via certified e-waste disposal providers.
- Paper records (if any) containing sensitive information must be stored in locked cabinets and shredded when no longer required.

Incident Reporting & Monitoring

- Any security breaches, unauthorised access, or suspicious activity must be reported immediately to the management team.
- Regular security audits and inspections will be conducted to ensure compliance with this policy.
- Employees must complete security awareness training on physical security measures at least once per year.

Compliance & Enforcement

- Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.
- Awaken Energy reserves the right to update this policy as required to address evolving security threats and regulatory requirements.