I.T Access Control Policy

AWAKEN ENERGY

The purpose of this Access Control Policy is to establish guidelines for managing and restricting access to Awaken Energy's information systems, ensuring that only authorised individuals can access sensitive data and resources. This policy aims to protect the confidentiality, integrity, and availability of business and customer information.

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

- Customer and business data stored in AWS and Salesforce
- API integrations
- IT infrastructure, software applications, and third-party tools
- Physical and remote access to company networks and systems

Access Control Principles

- **Least Privilege:** Access will be granted based on the minimum necessary privileges required for job responsibilities.
- **Role-Based Access Control (RBAC):** Access will be assigned based on job roles and responsibilities.
- **Separation of Duties:** No single individual should have unrestricted access to critical systems to prevent fraud or misuse.
- **Need-to-Know Basis:** Sensitive information will only be accessible to those with a legitimate business requirement.

User Access Management

- All access requests must be formally submitted and approved by the relevant department head.
- New user access is provisioned based on role requirements and reviewed periodically.
- Temporary access must have an expiry date and be monitored.
- Access to systems will be revoked immediately upon employee termination or role change.

Authentication & Identity Management

- Multi-Factor Authentication (MFA) is required for all critical systems, including AWS, Salesforce, and other sensitive platforms.
- Passwords must meet complexity requirements and be changed periodically.
- Single Sign-On (SSO) will be implemented where feasible to enhance security and usability.
- Failed login attempts will be monitored, and accounts may be locked after multiple failed attempts.

Remote Access Security

- Remote access to company systems must be conducted through company-approved VPNs.
- Devices accessing company systems remotely must comply with security policies and have endpoint protection installed.
- Access logs for remote connections will be maintained and reviewed periodically.

API & System Integration Access

- API access must be controlled using unique authentication tokens and secure encryption protocols.
- System-to-system integrations will be reviewed for security compliance before deployment.
- API rate limits and logging must be enforced to monitor unusual activity.

Monitoring & Review

- Regular access reviews will be conducted to ensure compliance with access control policies.
- Unauthorized access attempts will be logged and investigated.
- Security audits will be conducted periodically to identify access control vulnerabilities.

Compliance & Enforcement

- Non-compliance with this policy may result in disciplinary action.
- Employees must report any suspected security breaches or unauthorized access immediately.
- This policy aligns with industry best practices and regulatory requirements, including Australian Privacy Principles (APPs).