Information Classification Policy

AWAKEN ENERGY

The purpose of this Information Classification Policy is to establish a framework for classifying and managing information at Awaken Energy. This ensures appropriate handling, storage, access control, and protection of data in compliance with regulatory requirements and business needs.

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

- Customer data collected during sales processes
- API data exchanges
- Business operations and internal communications
- IT infrastructure, software, and digital assets
- Financial and compliance-related records

Classification Levels

All information assets at Awaken Energy are classified into four categories based on sensitivity and impact:

- **Public:** Information intended for public distribution (e.g., marketing materials, general website content).
- **Internal:** Non-sensitive business information available to all employees (e.g., operational guidelines, internal policies).
- **Confidential:** Sensitive business or customer data that requires controlled access (e.g., customer records, sales transactions, API logs).
- **Restricted:** Highly sensitive data with strict access control due to legal, financial, or regulatory requirements (e.g., personally identifiable information (PII), financial records, security credentials).

Information Handling & Protection Measures

- **Public Data:** May be shared externally with no restrictions.
- **Internal Data:** Accessible to all employees but should not be distributed externally without approval.
- **Confidential Data:** Requires access control, encryption during transmission, and storage in secured AWS and Salesforce environments.
- **Restricted Data:** Access granted only to authorised personnel. Must be encrypted at rest and in transit, with multi-factor authentication (MFA) required for access.

Roles & Responsibilities

- **Information Owners:** Classify and ensure appropriate protection measures for their data.
- **IT Security Team:** Implements technical controls and monitors data security.
- **Compliance Officer:** Ensures compliance with privacy regulations and industry standards.
- **Employees & Contractors:** Responsible for handling information according to classification guidelines.

Access Control & Data Sharing

- Access is granted based on the principle of **least privilege**.
- Sensitive and restricted information must not be shared through unsecured channels.
- API data exchanges must adhere to secure authentication and encryption protocols.

Data Retention & Disposal

- Data retention policies will be enforced based on classification level.
- Confidential and restricted data must be securely disposed of when no longer required, using approved data sanitisation methods.

Compliance & Monitoring

- Regular audits and security assessments will be conducted.
- Non-compliance with this policy may result in disciplinary action.