Data Security Policy

Purpose

This document defines the data security policy of A Energy Company. A Energy Company takes the privacy of our employees and clients very seriously. To ensure that we are protecting our corporate and client data from security breaches, this policy must be followed and will be enforced to the fullest extent.

Intent

The goal of this policy is to inform employees at A Energy Company of the rules and procedures relating to data security compliance.

The data covered by this policy includes, but is not limited to, all electronic information found in e-mail, databases, applications, and other media; paper information, such as hard copies of electronic data, employee files, and internal memos; etc.

Audience

This policy applies to all employees, management, contractors, vendors, business partners, and any other parties who have access to company data.

Data Types

A Energy Company deals with two main kinds of data:

1. Company-owned data that relates to areas such as corporate financials, employment records, payroll, proprietary information about our products, etc.
2. Private data that is the property of our clients and/or employees, such as Social Security numbers, credit card information, contact information, etc.

Data Classifications

A ^Energy Company data is composed of 4 classifications of information:

1. ***Public/Unclassified*** This is defined as information that is generally available to anyone within or outside of the company. Access to this data is unrestricted, may already be available, and can be distributed as needed. Public/unclassified data includes, but is not limited to, marketing materials, annual reports, corporate financials (and other data as applicable). Employees may send or communicate a public/unclassified piece of data with anyone inside or outside of the company.

2. ***Private*** This is defined as corporate information that is to be kept within the company. Access to this data may be limited to specific departments and cannot be distributed outside of the workplace. Private data includes, but is not limited to, work phone directories, organizational charts, company policies (and other data as applicable). All information not otherwise classified will be assumed to be private. Employees may not disclose private data to anyone who is not a current employee of the company.

3. ***Confidential*** This is defined as personal or corporate information that may be considered potentially damaging if released and is only accessible to specific groups (e.g., payroll, HR, etc.). Confidential data includes, but is not limited to, Social Security numbers, contact information, tax forms, accounting data, security procedures, and other personal data. A ^Energy Company considers it a top priority to protect the privacy of our clients and employees. A separate privacy policy outlines our commitment to protecting personal data. Employees may only share confidential data within the department or named distribution list.

4. ***Secret/Restricted*** This is defined as sensitive data which, if leaked, would be harmful to A ^Energy Company, its employees, contractors, and other parties as applicable. Access is limited to authorized personnel and third parties as required. Secret/restricted data includes but is not limited to audit reports; legal documentation; business strategy details; and proprietary information about designs, materials, and processes. Secret/restricted data cannot be disclosed by anyone other than the original author, owner, or distributor.

It is the responsibility of everyone who works at A [Energy] Company to protect our data. Even unintentional abuse of classified data will be considered punishable in accordance with the extent and frequency of the abuse.

Responsibilities

All employees are responsible for adhering to the policy and reporting any activities that do not comply with this policy.

Management personnel are responsible for ensuring that those who directly report to them understand the scope and implications of this policy. Human resources must also ensure that all employees have a signed copy of this policy in their file.

Security staff will be monitoring data for any unauthorized activity and are responsible for updating access requirements as needed.

Any employee who authors or generates corporate or client data must classify that data according to the criteria outlined above.

Management

Ownership of this policy falls to the IT team. For any questions about this policy, or to report misuse of corporate or personal data, please contact the IT team at ITteam@aenergycompany.com. The IT team will work to maintain data access privileges, which will be updated as required when an employee joins or leaves the company.

These are the accepted technologies A [Energy] Company uses to enforce and ensure data security:

1. Access controls
2. Strong passwords
3. System monitoring
4. Trend analysis

Review

Management is responsible for keeping this policy current. This policy will be reviewed annually or as circumstances arise.

Also annually, a full security audit will be performed by the IT team and selected company members to ensure that the policy is properly aligned with industry standards.

Enforcement

Employees found to be in violation of this policy by either unintentionally or maliciously stealing, using, or otherwise compromising corporate or personal data may be subject to disciplinary action up to and including termination.

Employee Acknowledgement

I agree to the terms and conditions set forth in this policy:

Employee Name: _____   **Date:** _____

Employee Signature: _____

Witness Name: _____   **Date**: _____

Witness Signature: _____