Organization Information Security Policy

Last Modified: MM/DD/YYYY

Last modified by: Name and department

Document changes:

Contents

Purpose

The purpose of this policy is to define the information security policies applicable to Organization that protect the confidentiality, integrity, and availability of data.

Scope

All employees and third-party users.

Information Security Policy

Principle

Information security is managed based on risk, legal and regulatory requirements, and business need.

Chief Executive Statement of Commitment

Information processing is essential to our success at Acme Co, and the protection and security of that information is our utmost priority. We have provided the resources to develop, implement, and continually improve an information security management system (ISMS) that is appropriate for our business and compliant with ISO 27001 standards.

Name: _____ Signature: _____ Date: MM/DD/YYYY

Introduction

Information security protects the information that is entrusted to Organization . Neglecting our responsibilities pertaining to information security can have significant adverse effects on our customers, employees, reputation, and finances. An effective information security management system enables Organization to:

- Provide assurances for our legal, regulatory, and contractual obligations
- Ensure the right people have the right access to the right data at the right time
- Protect personal data

Information Security Defined

Information security preserves:

- Confidentiality: Access to information is restricted to those with the appropriate authority
- Integrity: Information is complete and accurate at all times
- Availability: Information is available when needed

Information Security Objectives

To ensure the confidentiality, integrity, and availability of company information based on good risk management, legal, regulatory, and contractual obligations, and business needs.

To provide the resources required to develop, implement, and continually improve the information security management system (ISMS).

To effectively manage third-party vendors who process, store, or transmit information to identify, manage, and mitigate information security risks.

To create a culture of information security and data protection through effective employee training and risk awareness.

Information Security Policy Framework

The information security management system (ISMS) is built on an information security policy framework, which is made up of the following policies:

- Data protection policy
- Data retention policy
- Access control policy
- Asset management policy
- Risk management policy
- Information classification and handling policy
- Information security awareness and training policy
- Acceptable use policy
- Clear desk and clear screen policy
- Remote working policy
- Business continuity policy
- Backup policy
- Malware and antivirus policy
- Change management policy
- Third-party supplier security policy
- Network security management policy
- Information transfer policy
- Physical and environmental security policy
- Cryptographic key management policy
- Cryptographic control and encryption policy
- Document and record policy

Information Security Roles and Responsibilities

Everyone at Organization is responsible for understanding and adhering to established policies and processes, as well as for reporting any suspected or confirmed breaches. Specific roles and responsibilities regarding the information security management system (ISMS) are defined in the Information Security Roles and Responsibilities document.

Monitoring

Compliance with the policies and procedures of the information security management system are monitored by the Board of Directors, Mangement Review Team , together with periodic independent reviews by both internal and external auditors.

Legal and Regulatory Obligations

Organization takes its legal and regulatory obligations seriously. These requirements are recorded in the Legal and Contactual Requirements Register document.

Training and Awareness

Policies are made readily and easily available to all employees and third-party users. A training and communication plan is in place to communicate the policies, process, and concepts of information security. Training needs are identified, and relevant training requirements are captured in the Competency Matrix document.

Policy Compliance

Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by the CISO, CTO, Head of IT in advance and reported to the Management Review Team, Board of Directors .

Non-Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The policy is updated and reviewed on an annual, monthly basis as part of the process for continual improvement.