Information Security Policy

Purpose

The purpose of this policy is to establish an Information Security Program which protects the confidentiality, integrity, and availability of <Company Name>'s data and assets.

The program defines and implements safeguards that help <Company Name> prevent unauthorized access, disclosure, loss, or inappropriate use of data. It aims to ensure that data is protected, both during transmission and at rest, from internal, external, accidental, and deliberate threats.

Scope

The policy applies to all employees of <Company Name>, and all systems and data owned by it.

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

The Information Security Program institutes technical, physical, and administrative safeguards to protect data and assets from unauthorized access, disclosure, or inappropriate use. The program establishes requirements and standards, and organizes them into Policy documents. Policies encompass, but are not limited to the areas listed below.

Backup

<Company Name>'s backup procedures are documented in its Backup Policy. The purpose of this policy is to institute the necessary controls to mitigate the accidental loss of <Company Name> data. These controls assume that events such as accidental data corruption, deletion, or destruction will occur, and mitigate the impact of such events by maintaining reliable backup copies from which data can be readily restored.

Encryption

Encryption practices are documented in <Company Name>'s Encryption Policy. The purpose of this policy is to establish practices for protecting <Company Name> data in the event of unauthorized access through the use of encryption. The policy describes the different components that can be configured to utilize encryption, the algorithm that must be used for each, and how encryption keys should be managed.

Change Management

<Company Name>'s change management process is documented in its Change Management Policy. The purpose of this policy is to provide guidance on the process of managing change across <Company Name>'s critical systems and products in order to ensure that sufficient checks and balances are in place to mitigate the risks inherent in continuous product development.

Vulnerability Management

<Company Name>'s Vulnerability Management program is documented in the Vulnerability Management Policy. The purpose of this policy is to establish vulnerability management controls and provide guidelines for their implementation. Vulnerability management encompasses source code, operating systems, runtimes, and devices, and vulnerability scans are performed externally via penetration testing and web application scans.

Access Control

<Company Name>'s access control practices are documented in its Access Control Policy. The purpose of this policy is to establish the principles and guidelines for controlling access to systems owned by <Company Name>.

Authentication and Password

<Company Name>'s approach to authentication and password management is documented in <Company Name>'s Authentication and Password Policy. This policy describes <Company Name>'s requirements with regard to account authentication, including how passwords should be generated, used, and protected.

Security Incident Response

<Company Name>'s procedures for handling security incidents are documented in its Security Incident Management Policy. The purpose of this policy is to establish requirements and plans for reporting and responding to security incidents impacting <Company Name>'s corporate or customer systems.

Business Continuity

<Company Name>'s business continuity plan is documented in the Business Continuity Policy. The purpose of this policy is to establish requirements and plans to recover <Company Name>

operations following a disruption due to causes such as natural disaster, loss of access to premises, pandemic, or malicious activity from external or internal sources.

Risk Management

<Company Name> maintains a risk management program to identify, prioritize, and mitigate risk to acceptable levels.

The program consists of regularly performed risk assessments, which identify and prioritize security and compliance gaps, and recommend additional security controls needed to mitigate the risk carried by the gaps.

Policy Management

The company develops and maintains formal policies that govern information security within the company. The policies are formally reviewed and approved at least once a year, and are communicated to all employees.

Policy Creation

<Company Name><Company Name>'s management team is responsible for creating policies and supporting any relevant requirements and activities through sufficient staffing and budget allocation. The management team is also responsible for ensuring that <Company Name>'s staff is trained to understand and remain familiar with all relevant policies, and for keeping policies available for review both internally and externally by customers and partners.

Policy Reviews

[POLICY OWNER]

is responsible for ensuring all <Company Name> information security policies are reviewed at least annually by <Company Name> management, and re-approved or updated as necessary.

Existing policies may be updated and new policies may be created for reasons including:

- Complying with applicable laws and regulations
- Complying with new requirements for certification and governance by the company or its customers
- Addressing new threats
- Technological or business requirements

Policy Retention

As policies and procedures are updated over time to reflect the evolving nature of <Company Name> and its business, previous versions of these documents will be retained as dictated by compliance and legal requirements. For example, to comply with the Health Insurance

Portability and Accountability Act (HIPAA), policies and procedures are retained for up to six years.

Current and previous versions of <Company Name>'s policies and procedures are stored in its compliance management tool, Kintent. In addition, these policies and procedures are made freely available to all <Company Name> employees.

Security Awareness Training

Security awareness training is provided to new employees, and to all employees on a recurring annual basis, to promote strong security practices for the whole company.

All workforce members are required to complete Security Awareness Training shortly after they join the company and annually thereafter. In addition, they may be asked to complete further training as dictated by operational or environmental changes.

Changes that might lead to adjustment of the training program include:

- A security incident retrospective determining that additional training is required
- Adoption of new technology by the company
- Material changes in organizational policies

A record of the successful completion of each training session must be recorded for each employee. The record may be automatically collected by the training system, or manually gathered by the trainer. Records are retained for a period dictated by compliance and legal requirements.

[POLICY OWNER]

is responsible for creating the training program, and for selecting and updating training material over time. The program may be delivered internally, by qualified personnel, or by a third-party vendor.

Security Officer

Management and the Board of Directors consider requirements relevant to security, availability, processing integrity, and confidentiality. These considerations are documented in the company's Information Security Policy, which specifically delegates the overall responsibility of security to the Security Officer.

[POLICY OWNER]

is the designated Chief Information Security Officer at <Company Name>. As such, [POLICY OWNER]

is responsible for creating, approving, and enforcing security policies and procedures, leading the monitoring, vulnerability management, and incident detection and response initiatives, and tracking and reducing risk across the organization.

[POLICY OWNER]

and their supporting team are responsible for setting the direction of and taking the authoritative role in <Company Name>'s Information Security Program and related activities, including:

- Coordinating internal and external assessments
- Designing and implementing security controls
- Leading security incident response activities
- Monitoring systems and networks to detect vulnerabilities and misconfigurations, and to promptly resolve them
- Regular testing of all security controls