Important Note to User: This sample policy is not "one-size-fits-all" and should not be used by any organization without review and modification to fit the needs of such organization. Organizations should cross-reference with relevant existing policies where appropriate, comparing against relevant policies (e.g. mobile device and acceptable use policies), ensuring terms are defined consistently across policies. Additional changes to this policy may be necessary to account for varying individual organizational security needs and user privacy expectations. In addition, while efforts have been made to ensure that the terms of this policy comply with employee rights under the National Labor Relations Act, this is a contentious and eve- changing area of the law, and therefore total compliance cannot be guaranteed. **Delete this note before publishing.**

Sample Information Security Policy

Establishment date, effective date, and revision procedure

This policy was established and approved by [Organization Name] on [mm/dd/yyyy]. The [Organization Name] Information Security department shall review this policy at least once a year, and at any additional time when there are changes that may affect corporate management with respect to Information Security. In the event that amendment or repeal of this policy becomes necessary as a result of such review, the [Organization Name] Information Security department shall prepare a draft and apply for authorization, and with prior confirmation of the Executive(s) in charge of the area(s) that will be affected by amendment or repeal, the [Organization Name] CISO/Security Director will authorize the amendment or repeal.

Table of revision history

Version	Date	Details of change	Issued by	Approved by

Overview

Purpose

The purpose of this policy is to describe [*Organization Name*]'s commitment, and the commitment of its management, to preserving the confidentiality, integrity, authenticity, and reliability of business-related information and personal information in the possession or control of the company and/or any of its employees, agents, contractors, subsidiaries, or affiliates, through the establishment of a comprehensive information security program.

Scope

This policy applies to employees, contractors, consultants, volunteers, temporary and other workers at [*Organization Name*], and all personnel affiliated with company subsidiaries or third parties. This policy applies to all equipment that is owned or leased by, or otherwise in the custody or control of, [*Organization Name*].

This policy applies to the use of all information, electronic and computing devices, and network resources used by [*Organization Name*] to conduct business or interact with internal networks and business systems, whether owned or leased by, or otherwise in the custody or control of, [*Organization Name*], the employee, a company subsidiary, or a third party.

Definitions

Information Security: As used in this Policy, *information security* means the preservation of the confidentiality, integrity, authenticity, and reliability of information through safeguards designed to protect against any unauthorized access, use, modification, or disclosure.

Executive Management: As used in this Policy, *executive management* means all directors and officers of the organization.

Policy

[*Organization Name*] and its executive management recognize the importance of managing information security risk across all levels of the organization in a manner that aligns with organizational principles, goals, and business continuity and processes. Executive management will set the organization's risk tolerance and implement policies and procedures that effectuate the organization's information security interests and align with its risk appetite. Accordingly, policies and procedures will be enacted that address the following:

1. Management of all user IDs and passwords on IT Assets;
2. Management of all access control lists on all IT Assets;
3. Execution and review of all audit trails;
4. Incident response and reporting; and
5. All other tasks necessary to support this Policy.

[*If the organization handles protected heath information and is covered by HIPAA and its regulations, the following policies and procures should be included: Workforce Security and Information Access Management Policy; Sanction Policy; Information System Activities Review Procedures; Data Backup Plan; Disaster Recovery Plan; Emergency Mode Operations Plan; HIPAA Physical Safeguards Policy; and HIPAA Technical Safeguards Policy.*]

Executive management may enact additional policies and procedures in its discretion in order to provide the appropriate level of protection to business-related information in the possession or control of the company and/or any of its employees, agents, contractors, subsidiaries, or affiliates.

Framework of [*Organization Name*]'s Information Security Program

In order to effectively manage risk to information security, [*Organization* Name] will provide for the following safeguards:

1. *Access control and user authentication management.* Physical and technological access control will be implemented to provide only authorized users with access to sensitive business information, systems, and networks for legitimate business purposes.

2. *System and network monitoring*. All systems and networks will be monitored through review of access logs, activity logs, fault logs, and privileged operations in order to detect any suspicious activity that could signal internal abuse of access rights or the presence of an intruder.

3. *Ongoing assessment of information security risk*. Risk assessments will be conducted to identify newly developed or developing vulnerabilities in systems and networks and to determine what modifications if any should be made to existing information security safeguards. As part of such assessments, information classifications shall be reviewed to ensure such classes are appropriate for the level of risk associated with the information.

4. *Employee training and awareness*. All employees will be trained on basic information security such as recognition of social engineering schemes (e.g., phishing and spear phishing), ransomware, authorized uses and disclosures of information, and proper transmission, storage, and disposal/destruction of data. Employees will be responsible to secure transmission and storage of sensitive data through encryption or other appropriate means where required by data class or law.

5. *Compliance with legal obligations*. The information security program will provide an awareness of and comply with federal and state laws and contractual obligations including those related to protection of personal information.

6. *Vendor Management.* Whenever confidential or sensitive data is released to entities outside of the organization, and a legitimate business reason exists for releasing the information, a written Non-Disclosure Agreement (NDA), requiring the data recipient's agreement to maintain that data in confidence and restrict its use and dissemination, will be obtained before disclosing the data. Ongoing assessment of vendor relationships and vendor compliance with existing NDA's and other agreements will be conducted by the relevant vendor owners.

7. *Information security incident preparedness.* Detailed procedures will be in place to manage and direct the organization's response to an information security incident including designation of an Incident Response Team and the role of each team member.

8. *Business Continuity Plan*. Information security will be coordinated to effectuate and further the goals of the organization's business continuity plan.

9. *Sanctions for violations*. Appropriate warnings or disciplinary action will be brought against any employee, agent, contractor, or affiliate of the organization who violates the terms of any of the organizations information security policies, including possible termination of employment or expulsion from the organization's premises.

Additional safeguards may be necessary to protect assets of greater criticality, or where, after conducting a risk assessment, it is determined that the current information security program is insufficient to protect the organization's information, systems, and/or networks commensurate with the organization's risk tolerance.

Information Security Roles and Responsibilities

Information Security will be primarily managed by [*Organization Name*]'s Chief Information Officer, Chief Information Security Officer, and Information Technology personnel [*or other persons with similar roles*]. Individual department managers will be responsible for ensuring that employees within their departments are complying with [*Organization Name*] information security policies and procedures. Responsibilities of those in information security roles will include:

1. Fostering an organizational climate where information security is prioritized and considered in the context of business continuity and objectives.

2. Defining the security requirements, controls and mechanisms applicable to all covered data.

3. Defining the methods and guidelines used to identify and classify all covered data.

4. Defining the procedures for identifying data owners for all covered data.

5. Defining the labeling requirements for all covered data.

6. Defining all other data security usage, processing, transmission, storage and disposal processes and procedures.

7. Assisting department managers and supervisors to better understand how information security risks associated with their systems translate to organization-wide risk.

8. Providing ongoing assessment of the risk to the organization's information, systems, and networks.

9. Monitoring the organization's systems and networks for questionable activity.

10. Defining the procedures necessary to ensure compliance to this policy by all organization users and vendors.

11. Ensuring all members of executive member remain apprised of the organization's information security posture and any developing risks.

12. Assisting in the organization's ongoing compliance with state and federal law and other legal obligations.

13. Working with other Incident Response Team members to respond to, contain, and eradicate information security incidents.

Policy Compliance

Compliance Measurement

Compliance with this policy will be verified by the [*Organization Name*] 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 by the [Policy Owner] in advance.

Non-Compliance

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

By signing below, I acknowledge that I have read and fully understand my obligations under this Policy and hereby agree to abide by its terms.

_____ _____

Name Date