Data Security Policy – Security Management

PURPOSE

To provide principles and guidelines for managing Organization's information security program and processes.

SCOPE

The Security Management Policy will cover Organization's:

- Information Security Management policy and program
- Security program documentation, including creation and retention
- Organizational structure
- Risk management activities, treatment, and assessments
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has defined a security management process that incorporates a risk-based approach, and takes into account the resources, both internal and external, available to the company. Organization considers information security a priority and has established controls and processes to keep sensitive information and protected information, such as ePHI, safe.

In addition to specific processes and controls, Organization's leadership, including senior management and the Board of Directors, are committed to a security-conscious company culture, and information security.

Information Security Management Program

Organization's information security program defines roles and responsibilities for personnel. Charts, policies, and procedures reflect the responsibilities of the Board of Directors, the independence of the Board, and the expertise available on the Board.

Organization has based its information security program on frameworks and best practices that support its objectives, including relevant accounting standards and the Center for Information Security (CIS). The company's information security program considers the regulatory and compliance standards that need to be included in the program, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Organization's information security program ensures that controls and processes maintain the confidentiality, integrity, and availability (the CIA triad) of sensitive or protected data. When needed, the company separates incompatible duties between different personnel or roles.

Organization Chart

Organization has an organization chart that lists personnel and their roles and/or titles and includes reporting lines. The organization chart is reviewed and updated at least annually, or when significant changes occur.

Compliance Documentation and Retention

For compliance and analysis purposes, all control activities related to information security are documented. This documentation may need to be provided for audit and assessment purposes. Documentation is a key step in any control activity and should always be completed thoroughly. Electronic documentation, audit logs, ticketing systems, and other IT systems assist with collecting this type of documentation and information. Access to documentation repositories is limited to appropriate personnel only, as it may contain sensitive or protected information.

Risk Management

Organization applies risk management principles to its information security program in order to better identify, assess, and address risks or threats to the company. Information security risk management involves a cycle of steps:

1. Risk Identification
2. Risk Analysis
3. Risk Treatment and Action Plan
4. Risk Monitoring and Review

Risk assessments are an important part of our risk management program and are performed at least annually. The Guard's data security program is available as one tool in this assessment and includes evidence collection and risk assessment components.

The company’s risk register is also reviewed and updated at least annually and includes any findings from completed risk assessments.

Risk Register

A risk register is a document or database that contains a listing of the company’s risks, including:

- Risk description
- Risk likelihood score
- Risk impact score
- Risk analysis (aggregated score, usually calculated as likelihood score * impact score)
- Risk treatment
- Risk action plan or remediation plan, including an estimated date of completion
- Risk owner
- Other relevant notes or data points

Risk Committee

Organization has created a Risk Committee and an accompanying Charter that outlines the Risk Committee’s purpose, objectives, and required deliverables or outcomes. The Risk Committee meets at least quarterly, and documents meeting minutes that we retain for compliance purposes. If necessary, the risk register should be updated to reflect updates and changes following the Risk Committee meeting.

ROLES AND RESPONSIBILITIES

Risk Committee: Meets quarterly to review the company’s risk posture, including the risk register and any recent risk assessments. Provides cross-functional insights into risk management. Decides the priority of risks as needed.

VIOLATIONS

Violations of the information security policy and program may be subject to disciplinary action.

FORMS/PLANS/DOCUMENTS

- Organization Chart
- Risk Committee Charter
- Risk Committee Meeting Minutes
- Risk Assessment Documentation

RELEVANT HIPAA REGULATIONS

- [§164.308(a)(1)(ii)(A)](https://www.ecfr.gov/cgi-bin/text-idx?node=pt45.2.164&rgn=div5 *Risk analysis*
- [§164.308(a)(1)(ii)(B)](https://www.ecfr.gov/cgi-bin/text-idx?node=pt45.2.164&rgn=div5 *Risk management*
- [§164.308(a)(1)(ii)(C)](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164 *Sanctions Policy*
- [§164.308(a)(1)(ii)(D)](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164 *Information system Activity Review*

RELEVANT SOC 2 CRITERIA

- CC1.1.1 *Sets the tone at the top*
- CC1.2.1 *Establishes oversight responsibilities*
- CC1.2.2 *Applies relevant expertise*
- CC1.2.3 *Operates independently*
- CC1.2.4 *Supplements board expertise*
- CC1.3.1 *Considers all structures of the entity*
- CC1.3.2 *Establishes reporting lines*
- CC1.3.3 *Defines, assigns, and limits authorities and responsibilities*
- CC1.3.4 *Addresses specific requirements when defining authorities and responsibilities*
- CC3.1.1 *Reflects management's choices*
- CC3.1.2 *Considers tolerances for risk*
- CC3.1.3 *Includes operations and financial performance goals*
- CC3.1.4 *Forms a basis for committing of resources*
- CC3.1.5 *Complies with applicable accounting standards*
- CC3.1.6 *Considers materiality*
- CC3.1.7 *Reflects entity activities*
- CC3.1.8 *Complies with externally established frameworks*
- CC3.1.9 *Considers the required level of precision*
- CC3.1.10 *Reflects entity activities*
- CC3.1.11 *Reflects management's choices*
- CC3.1.12 *Considers the required level of precision*
- CC3.1.13 *Reflects entity activities*
- CC3.1.14 *Reflects external laws and regulations*
- CC3.1.15 *Considers tolerances for risk*
- CC3.1.16 *Establishes sub-objectives to support objectives*
- CC4.2.1 *Assesses results*
- CC4.2.2 *Communicates deficiencies*
- CC5.1.1 *Integrates with risk assessment*
- CC5.1.2 *Considers entity-specific factors*
- CC5.1.3 *Determines relevant business processes*
- CC5.1.4 *Evaluates a mix of control activity types*
- CC5.1.5 *Considers at what level activities are applied*
- CC5.1.6 *Addresses segregation of duties*
- CC5.3.1 *Establishes policies and procedures to support deployment of management's directives*
- CC5.3.2 *Establishes responsibility and accountability for executing policies and procedures*