**COMPANY Logo**

Information Security Program Mission & Information Security Organization Charter

Effective Date:

**COMPANY Logo**

Revised:

Approved by: CISO Approved on: 00/00/20XX

Approved by: CEO Approved on: 00/00/20XX

Approved by: Board of Directors Approved on: 00/00/20XX

# Introduction

Information is one of COMPANY (“COMPANY” or the “firm”) most important assets.

Protection of information assets is necessary to establish and maintain trust between COMPANY and its customers, maintain compliance with the law, and protect its business reputation. The security of COMPANY’s systems and information is essential to the privacy of customer financial and non-public information.

Information security is the method by which COMPANY protects and secures the systems, media, and facilities that process and maintains information vital to its operations. Security is an ongoing process, whereby the condition of COMPANY’s controls is just one indicator of its overall security posture.

COMPANY believes an effective Information Security Program is one that continuously integrates processes, people, and technology to mitigate risk in accordance with the firm’s risk assessment and acceptable risk tolerance levels. In order for the Information Security Program to be successful, it must:

* receive a strong level of support from the Board of Directors and Senior Management
* integrate security activities and controls throughout business processes
* establish clear accountability for carrying out security responsibilities

COMPANY’s Information Security Mission Statement:

***We will protect client and company information, provide proactive security analysis, maintain robust security architecture and ingrain security awareness into the company’s culture.***

# Information Security Program Mission

COMPANY’s Information Security Program’s mission is to provide quality information security technology and services which make a recognizable contribution to our business and enhance the value of our organization to the industry. The Information Security Program provides a core set of policies in the Information Security Policies to ensure the control, reliability, integrity, availability and protection of corporate information (both electronic and paper) used enterprise-wide by COMPANY.

The information created, processed, and used by COMPANY is one of our most valuable assets. Given the competitive nature of our business and market dynamics, these assets must be protected commensurately with how their loss will impact COMPANY’s business. The compromise of these assets could severely impact our business, constitute a breach of laws and regulations, and at the very least negatively affect COMPANY’s credibility and brand image.

All information, documents, and material to which our staff are exposed by virtue of employment with COMPANY are property of COMPANY. If our competitors are somehow able to obtain this information, we lose our investment in time and money, and they may gain an unfair business advantage, which in time could hurt COMPANY. In addition, with respect to Non-Public Information (NPI), the compromise of this information could have legal ramifications.

In order to safeguard this information from unauthorized disclosure, COMPANY requires that specific protective measures be taken. We take protection of this information seriously and expect all staff to also take its protection seriously. The framework for the COMPANY Information Security Program is based on the International Standards for Information Security (ISO) 17799 and 27002.

The Information Security Program is sponsored by the Chief Operation Officer (COO) or CEO. The Information Security Organization performs the management function and conducts overseeing activities associated with the Information Security Program.

# Information Security Organization Charter

The purpose of this charter is to establish the governance and resources for the Information Security Organization.

The Information Security Organization has enterprise level responsibilities to develop Information Security Policies, Standards & Procedures, and define roles and responsibilities to manage how information security issues are handled by COMPANY. These roles are assigned by the Information Security Organization.

The Information Security Organization evaluates the adequacy and effectiveness of information security and information protection controls for business processes which handle and manage non-public information, and ensures corporate compliance with applicable information protection laws and regulations.

# Scope of Activities

The Information Security Organization’s scope of activities includes:

* Developing and maintaining the Information Security Policies, Standards, Procedures, and Guidelines.
* Developing and maintaining Information Security Awareness materials.
* Interacting with Businesses and Organizations through-out COMPANY to identify, implement, and design information security and privacy requirements, controls, and safeguards.
* Ensuring the protection of privacy of non-public information.
* Assisting management in defining Information Classification Levels.
* Creating a security plan, which includes both strategic (e.g., long-term projects that may not be realized for 6 – 12 months) and tactical (e.g., projects that require immediate implementation) planning initiatives.
* Gathering and monitoring security metrics to assist in the measurement and analysis against the information security plan.
* Defining, evaluating, selecting and acquiring security technologies, methods, and practices for utilization within the COMPANY information technology infrastructure.
* Monitoring vulnerability bulletins and defining processes to ensure identified vulnerabilities are evaluated and fixes are tested and implemented.
* Implementing incident response capabilities, including developing and maintaining an incident response plan and procedures.
* Certifying applications prior to deployment into production.
* Maintaining information security operations such as monitoring and intrusion detection and reviewing the administration of user accounts, access controls, firewall rule changes, and other administrative duties applicable to information security.
* Verifying compliance with Information Security Policies and Standards.

# Communication

The Information Security Organization will communicate the results of their activities to the COO, Legal, and Internal Audit Organizations as well as the Governance Team, both during and upon completion of the information security and information privacy processes. The Organization’s preliminary observations, recommendations and conclusions shall be discussed and reviewed with management prior to the issuance of final reports to ensure accuracy and clear communication.

The Information Security Organization will communicate regularly with and illicit participation from all Organizations and Businesses throughout COMPANY.

# Business Participation

Involvement of Businesses will cultivate an environment of cooperation in the achievement of information security goals. It will allow Businesses a perspective of the value of and services provided by the Information Security Program and Information Security Organization.

Businesses will articulate information security and protection needs, define requirements, and convey information protection concerns. This will allow Business Managers and the Information Security Organization to review information security risks; for the Business Managers to fully understand, and in some cases formally accept the risks.

# Authority

The COMPANY Information Security Program is managed by the Information Security Organization, with inputs from the IT, Legal, and Internal Audit Organizations as well as the Governance Team.

The Information Security Organization is authorized to:

* Access all relevant functions, records, property and personnel as needed in executing its responsibilities.
* Allocate resources within project teams and obtain the necessary assistance from personnel in key functional areas where they can provide key input to supporting decisions to process design and implementation efforts.
* Create methodology and initiate enterprise-wide process designs.
* Implement controls as defined by the Information Security Program.

# Information Security Responsibilities

The Information Security Organization shall have the responsibility to:

* Develop and maintain an Information Security Program – framework based on ISO 17799 and 27002 and ensuring adequate information security controls. This Information Security Program will include a policy and controls hierarchy, Information Security Polices, roles and responsibilities, and governance. The program will include identifying resources, developing and implementing supporting components, and conducting periodic assessments. As needed, the program is modified to reflect changing business risks or special projects which are appropriate and relevant to the mission of this Charter, with the approval of the Information Security Organization.
* Ensure consistent creation and implementation of information protection, privacy, and security relevant policies, standards, procedures, and guidelines.
* Identify Information Classification Levels and develop and maintain information handling and protection guidelines.
* Designate Information Security resources and contacts required to sign-off on regulatory requirements, as well as formal assignment of roles and responsibilities.
* Design, implement, and maintain the corporate-wide security architecture.
* Develop a formal inventory of systems and processes that involve transfer and protection of customer non-public information (including third parties).
* Develop and maintain Information Security Awareness materials.
* Identify long-term security strategy and design to enable business requirements and endeavors.
* Monitor vulnerability bulletins and defining processes to ensure identified vulnerabilities are evaluated and fixes are tested and implemented.
* Develop and maintain an incident response plan and procedures.
* Develop an application development security certification process.
* Collect and maintain security related metrics.
* Perform and supervise security operations such as the monitoring of firewalls and intrusion detection systems, review of audit logs, and user and administrator account management.
* Work with Internal Audit to perform annual assessments to applicable regulatory and legal information security requirements.
* Work with the Governance Team to validate compliance to Information Security Policies and Standards.

# Chief Information Security Officer (or equivalent)

The Chief Information Security Officer (CISO) is the primary evangelist for information security within COMPANY. It is the role of this individual to set primary strategic direction for COMPANY with respect to information security and business resumption, and to promote security awareness among senior executives within COMPANY.

The Chief Information Security Officer’s accountabilities are as follows:

* Setting strategic direction for information security throughout COMPANY.
* Promoting security awareness among COMPANY’s Executive and Senior Management.
* Developing an information security business plan.
* Coordination of information security activities throughout COMPANY.
* Corporate-wide information security risk assessment and adjudication.
* Promoting information security awareness within COMPANY.
* Providing the appropriate tools and metrics to business management to properly measure the state of information security within COMPANY.

The Chief Information Security Officer is used as the focal point for corporate-wide information security risk assessment and adjudication. The Chief Information Security Officer is an active participant in the security process, having influence concerning information security for both the central security functions within COMPANY and for each of the Businesses.

# Information Security Organization Roles

The Information Security Organization roles include the following:

Security Operations

* Audit Log Reviews
* IDS/Firewall Monitoring
* Audit Access Permissions
* User account management
* Platform administration
* Security permissions
* Email monitoring
* Internet site monitoring

Security Engineering

* Configuration Guidelines
* Vulnerability Bulletins
* Security Design and Infrastructure
* Incident Response Plan, Procedures and Capabilities
* Implementation and Maintenance
* Application Security Certification

Security Architecture

* Information Security Policies and Standards
* Strategy
* Information Classification
* Information Security Awareness & Training
* Business Requirements and Interactions
* Collect and Maintain Security Metrics
* NPI Privacy Compliance
* Regulatory Compliance
* Governance

# Information Security Program

The Information Security Organization provides the management and oversight activities associated with the Information Security Program. Senior Management sponsorship for the program is by the Chief Operation Officer (COO). IT, Legal, and Internal Audit Organizations as well as the Governance Team will provide input to and interact with the Chief Information Security Officer and the Information Security Organization as necessary for the establishment, management, and governance of the Information Security Program.

