**Company Logo**

Information Security Policy Master Plan

Effective Date:

**Company Logo**

Revised:

Approved by: Approved on: 00/00/0000

Approved by: Approved on: 00/00/0000

# Introduction

# COMPANY (“COMPANY” or the “firm”) ability to efficiently and effectively create, collect, process, manage, control, and use business information assets has a direct and increasing effect on all COMPANY business results and future performance.

# It must be ensured that all COMPANY information is protected to a level, which adequately reflects the business risk from unauthorized access, disclosure, modification or loss, and takes into account its value to COMPANY and its criticality or sensitivity. In addition, it must be ensured that COMPANY complies with all international, federal, and local laws and regulations.

# Information Security Policies are the foundation for all information security, privacy, and data protection efforts. In order to be successful an Information Security Program must have a set of Information Security Policies which establishes both direction and management support to ensure the control, reliability, integrity, availability and protection of corporate information (both electronic and paper) used enterprise-wide by COMPANY (“COMPANY” or the “firm”).

# Information security policies are used as a reference for all aspects of the Information Security Program, including such activities as designing security into applications, defining user access privileges, conducting threat and risk analysis, planning incident response, business continuity and disaster recovery, and disciplining staff for security violations. Since Information Security Policies have such an important and pervasive impact on all facets of an Information Security Program, it is essential that the policies are clear and easy to understand, relevant to COMPANY business needs and environment, enforceable by technical and process methods, and are implementable by the business.

# COMPANY’s Information Security Policies should be the basis for all other security documentation developed.

# Scope

# Information Security Policies apply to all Users (employees, contractors, vendors, consultants, and all other persons) having access to COMPANY computing assets or information. The term “users” generally means those persons employed by COMPANY. Throughout the Information Security Policies when the use of COMPANY computing assets is being addressed, the term “user” includes employees, contractors, vendors, consultants, and all other persons having access to COMPANY computing assets or information.

# Information Security Policies exist to protect COMPANY information network and infrastructure and apply to all COMPANY computing assets and information regardless of the controlling department or entity.

# Overview

# Information and Information Technology Systems are business assets of COMPANY and as such, everyone is responsible for their protection, accuracy, and availability (i.e., protecting from unauthorized access, use, modification, disclosure, etc.). All individuals with access to business information assets must use due care. Minimum standards of due care are in the Information Security Policies.

The Information Security Policies set forth a course of action for the protection of information assets at COMPANY to facilitate the need for a secure business environment. Growing interconnection with third parties, increasing market competition, and the widespread use of networking technologies make the protection of information critical to COMPANY’s business. Information must be protected so that it is not stolen, lost, destroyed, altered without authorization, or unavailable to authorized users. COMPANY must take measures to protect information assets from both internal and external threats.

# All Users of COMPANY information assets must comply with the following general business information security, privacy, and data protection requirements:

# Users must value and protect information as any other business asset.

# Users must understand that COMPANY’s ability to efficiently and effectively create, collect, process, manage, control, and use business information assets has a direct and increasing effect on all COMPANY business results and future performance.

# Users must understand how effective management of critical business information assets affects COMPANY’s business growth; ability to comply with laws and regulations; and public, customers, partners, and third party associate’s trust.

# Users must follow Information Security Policies, Standards, Procedures, and Guidelines to ensure that business information assets are managed and controlled so that only properly identified individuals with authorization can access the information.

# Users must follow implemented management controls and processes to ensure the continued productivity of business information assets in producing business results.

# Users must identify and sufficiently protect the most critical business information assets (including Non-Public Information).

# Users must understand the risk to critical business information assets if they are lost, stolen, altered, destroyed, or made unavailable.

# Users must understand threats to critical business information assets.

**Figure 1, Risk to Information and Business Impact**, depicts how internal and external threats will impact business information assets and thereby impact COMPANY’s business.



**Figure 1. Risk to Information and Business Impact**

COMPANY has a wide spectrum of business information assets. Information, considered in the broadest sense, includes, but is not limited to:

a) Customer Non-Public Information

b) Intellectual property

c) Personnel or human resources information

d) Earnings and financial information

e) Sales, marketing, and business plans and initiatives

f) Audio, visual, written, and electronic recordings

g) Client and partner information

h) Supply chain, manufacturing, and distribution information

i) Consulting, partnerships, contracts, out licensing, or acquisitions information

# Objectives

# The intent of the Information Security Policies is to identify at the highest level “what needs protection” and “what protection measures need to be taken”. The Information Security Policies will state the views, objectives, rules, and practices with respect to information security, privacy, and the control of how information and information resources are managed, protected, and used by both technical and non-technical controls and processes. All Users (employees, consultants, and contractors, including temporary employees) with access to information and information resources are responsible and accountable for adhering to the Information Security Policies.

COMPANY’s Information Security Policies are designed to accomplish the following primary objectives:

* Availability - The ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information or systems.
* Integrity of Information and Systems - System and information integrity relate to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.
* Confidentiality of Information and Systems - Confidentiality of information and systems covers the processes, policies, and controls used to protect customer and COMPANY information and systems against unauthorized access or use.
* Accountability - Clear accountability involves the processes, policies, and controls necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.
* Assurance - Assurance addresses the processes, policies, and controls used to develop confidence that technical and operational security measures work as intended. Assurance levels are part of the system design and include availability, integrity, confidentiality, and accountability. Assurance highlights the notion that secure systems provide the intended functionality while preventing undesired actions.

# Structure

The Information Security Policies provide high-level statements that describe the information protection goals and requirements of COMPANY. **Figure 2, Information Security Policy Structure**, depicts how the Information Security Policies, Standards, and other documents relate to each other. The information security and privacy practices defined in the Information Security Policies, Standards, Procedures, and Guidelines provide detailed control requirements for achieving the goals defined in this Information Security Policies Master Plan. COMPANY can use the specific Information Security Policies documents to measure compliance with information security policies.



# Figure 2. Information Security Policy Structure

# Information Security Policies

# The specific information security policies will be contained in the Information Security Policies as described below:

# Information Security Management

# Management Commitment

# Development & Maintenance of Information Security Policies

# Information Security Organization

# Security Coordination

# Roles and Responsibilities

# External Parties

# Risk Management

# Strategy

# Risk Analysis

# Risk Measurement

# Risk Control

# Governance

# Legal and Regulatory

# Third Parties and SLAs

# Information Security Policies

# IT

# Information Asset Management

# Information Ownership

# Information Classification

# Information Labeling

# Information Protection

# Cryptographic Controls

# Information Disposal

# Inventory of Information Assets

# Personnel Management

# Personnel Practices

# Acceptable Use

# Security Awareness and Training

# Termination

# Physical & Environmental Management

# Secure Facilities

# Entry Access

# Environmental

# Device Security

# Media and Hardcopy Handling

# Secure Work Areas

# Removal of Equipment

# Secure Disposal or Reuse of Equipment

# Equipment Maintenance

# Mobile Device Management

# Physical Security

# Logical Security

# Malware Protection

# Performing Backups

# Mobil Computing and Communications

# Telecommuting / Teleworking

# Access Control Management

# User

# Access Controls

# Identification and Authentication Controls

# Privilege Management / Authorization Controls

# User Password Management

# Password Controls Standard

# Administrator

# Policy

# Credential Management

# Network Access Control

# Operating System Access Control

# Application and Database Access Control

# Remote Access Control

# Security of Remote Devices

# Internet / VPN Access

# Dial-In / Modem Access

# Wireless Access

# Computer and Network Operations Management

# Operational Procedures

# System Planning and Acceptance

# Computer and Network Security

# Protection against Malicious Software

# Backups and Recovery

# Patches and Updates

# Vulnerability Management

# Oversight

# Identification

# Testing

# Analysis

# Remediation

# Metrics

# Monitoring Management

# Monitoring and Logging

# Review of Logs

# Log Protection

# Security Incident & Event Management

# Plan & Procedures

# Reporting

# Response

# System & Software Lifecycle Management

# Security Requirements

# Correct Processing

# Lifecycle Management

# Separation of Development, QA, Test, and Production Environments

# QA and Test

# Protection of System Files

# Change Controls

# Business Continuity & Disaster Recovery Management

# Planning

# Testing

# Maintenance

# Information Security Standards, Procedures & Guidelines

The following table identifies a representative list of Information Security Standards, Procedures and Guidelines associated with the Information Security Polices.

|  |  |  |  |
| --- | --- | --- | --- |
| **Policies** | **Policy Owners** | **Related Documents** | **Documents Owners** |
| Information Security Management | User Name | 1. Vendor Management Plan  2. Vendor Management Procedures  3. Project Management Procedures  4. Policy, Standards & Procedures Management Procedure | 1. User Name  2. User Name  3. User Name  4. User Name |
| Information Asset Management | User Name | 5. Special System Administration & Management Procedures  6. Data Labeling, Protection, and Disposal  7. Database Administration & Management Procedures  8. Encryption Administration and Management Standard  9. Managed Assets Administration & Management Procedures | 5. User Name  6. User Name  7. User Name  8. User Name  9. User Name |
| Personnel Management | User Name | 10. Company Policies  11. Place Holder  12. Code of Ethics  13. Place Holder  14. Place Holder  15. Place Holder  16. Place Holder | 10. User Name  11. User Name  12. User Name  13. User Name  14. User Name  15. User Name  16. User Name |
| Mobile Device Management | User Name | 17. Instant Messaging Administration & Management Standard  18. PDA Usage Administration and Management Standard  19. PDA Usage Administration and Management Procedures | 17. User Name  18. User Name  19. User Name |
| Access Control Management | User Name | 20. Disaster Recovery for Primary Systems  21. Password Standard  22. Telecommuting Guidelines  23. Third Party Access Standard  24. User Account Management Standard and Procedures | 20. User Name  21. User Name  22. User Name  23. User Name  24. User Name |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policies** | **Policy Owners** | **Related Documents** | **Document Owners** |
| Computer & Network Operations Management | User Name | 25. AD Configuration Standard  26. Anti-Virus Administration & Management Procedures  27. Special System Administration & Management Procedures  28. Backup and Restoration Standard  29. Managed Assets Administration & Management Procedures  30. IT Change Management Procedures  31. Database Administration & Management Procedures  32. Desktop/Laptop Administration & Management Procedures  33. Desktop and Laptop Configuration Standard  34. Data Loss Prevention Standard  35. Firewall Appliance Standard and Firewall Administration & Management Procedures  36. Help Desk Ticketing System Administration and Management Procedures  37. IDS Administration & Management Procedures  38. Laptop Administration and Management  39. Online Client Support Administration & Management Procedures  40. Phone Switch Administration & Management Procedures  41. Printer & Copier Administration & Management Standard  42. Printer & Copier Administration & Management Procedure  43. Remote Access Administration & Management Standard  44. Router & Switch Administration & Management Standards and Procedures  45. Server Administration & Management Procedures  46. Network Connectivity/Wireless Management Procedures  47. VoIP Standard  48. Web Application Server Administration & Management Procedures | 25. User Name  26. User Name  27. User Name  28. User Name  29. User Name  30. User Name  31. User Name  32. User Name  33. User Name  34 User Name  35. User Name  36. User Name  37. User Name  38. User Name  39. User Name  40 User Name  41. User Name  42. User Name  43. User Name  44. User Name  45. User Name  46. User Name  47. User Name  48. User Name |
| Vulnerability Management | User Name | 49. Security Vulnerability Testing Procedures | 49. User Name |
| Monitoring Management | User Name | 50. IDS Administration and Management Procedures  51. Event Monitoring Administration and Management Standard  52. Audit Log Review Procedures  53. Event Monitoring Procedures  54. Audit Log Review Standard | 50. User Name  51. User Name  52. User Name  53. User Name  54. User Name |
| Security Incident & Event Management | User Name | 55. Incident Response Plan | 55. User Name |
| System & Software Lifecycle Management | User Name | 56. Secure Coding Standards  57. Application Assessment Procedures  58. Web Application Development Procedures  59. Web Application Server Administration and Management Procedures | 56. User Name  57. User Name  58. User Name  59. User Name |
| Business Continuity & Disaster Recovery Mgmt | User Name | 60. Disaster Recovery Response Procedures  61. Incident Response/Crisis Management Plan  62. BCP / DR Plans | 60. User Name  61. User Name  62. User Name |
| Physical Management | User Name | 63. Physical Security Standard | 63. User Name |

# Policy Enforcement

Information security and privacy must be supported throughout COMPANY, including by the Board of Directors, Senior Management, Users, and service providers. Each role has different responsibilities for information security and privacy and each individual is accountable for their actions. Accountability requires clear lines of reporting, clear communication of expectations, and the delegation and judicious use of appropriate authority to bring about appropriate compliance with COMPANY’s Information Security Policies, Standards, Procedures, and Guidelines.

# All COMPANY Managers are responsible for pro-actively enforcing the Information Security Policies Standards, Procedures, and Guidelines.

# Policy Governance

Governance is achieved through the management structure, assignment of responsibilities and authority, establishment of the Information Security Policies, allocation of resources, monitoring, and accountability. Governance is required to ensure that tasks are completed appropriately, that accountability is maintained, and that risk is managed for the entire enterprise.

The Information Security Policies exist to protect COMPANY’s overall information network and infrastructure and must be adhered to. Fulfillment of information security and privacy responsibilities is mandatory. Failure to do so may serve as a basis for disciplinary action including discharge. Periodic audits of activities by Internal Audit and the Governance Team will be used to verify compliance.

Individuals who violate systems or network security may incur criminal or civil liability. COMPANY will cooperate fully with investigations of violations of systems or network security, including cooperating with law enforcement authorities in the investigation of suspected criminal violations.

# Information Classification

Information is classified according to its potential impact on COMPANY. Information is either Public or Non-Public, with Public information being freely distributed internally and externally to COMPANY. Public Information is that which Users can disclose to anyone without violating an individual’s right to privacy or COMPANY’s proprietary rights or trade secrets, such as marketing brochures, business cards and press releases.

The following are Non-Public categories of information maintained by COMPANY:

* **Internal Use** Information is to be shared only with COMPANY Users, such as employee contact information, organizational charts, memoranda or communications marked “for internal use only” and non-technical policies and procedures.
* **Confidential** Information is intended solely for use within COMPANY and limited to those with business “need-to-know” such as personnel information, customer or consumer information, business unit and firm plans or non-public information, technical policies and system configuration guidelines.
* **Restricted** Information is intended solely for restricted use within COMPANY and limited to those with an explicit, predetermined, strategic “need-to-know” such as strategic plans, passwords, and encryption keys.

Users should not disclose Internal Use, Confidential or Restricted Information to Users who are not authorized with a proper “need-to-know”. Users should always verify the identity and the “need-to-know” status of anyone requesting Internal Use Only, Confidential and Restricted Information, and should notify their supervisors/managers of unauthorized attempts to obtain information.

The *Information Classification and Protection Guide* identifies and defines the information criticality, the sensitivity of information, “need to know” criteria and defines a set of information classification levels to be used by COMPANY. Based on the classification levels, information protection guidelines are defined for:

* Access Reviews
* Application Access
* Approval to Generate
* Copying or Reproduction
* Destruction - Hard Copy Documents
* Destruction - Magnetic Media
* Disclosure
* Electronic Transmission – Internal
* Electronic Transmission - External
* Encryption Requirements
* Fax Usage (External)
* Labeling
* Logging
* Mailing - Internal
* Mailing - External
* Meetings, Conferences, and Discussions
* Mobile Devices
* Reproduction
* Storage - Hard Copy Documents
* Storage - Electronic
* Telecommuting / Traveling
* Telephone Usage
* Unattended Desk / Office

# Roles and Responsibilities

All individuals with access to business information assets (COMPANY employees, contractors, consultants, vendors, business partners, or temporary employees) are responsible for the handling and protection of business information assets. The following roles have information security, privacy, and data protection responsibilities:

* **Chief Operations Officer (COO) or Chief Executive Officer(CEO)** is the Information Security Program Sponsor and is responsible for providing leadership for information security and privacy initiatives and funding.
* **Chief Information Security Officer (CISO)** is responsible for determining the potential business threats, risk, and vulnerabilities and ensuring information security is integrated throughout COMPANY. This includes:
  + - establishing an Information Security Program
    - setting strategic direction for information security, privacy, and data protection throughout COMPANY
    - developing an information security business plan
    - developing and maintaining Information Security Policies, Standards, Procedures, and Guidelines
    - defining information classification levels with associated protection controls and guidelines
    - establishing an Information Awareness and Training program
    - ensuring COMPANY has an effective Incident Response Team
    - ensuring adequate business continuity and disaster recovery planning and testing
    - providing security engineering support as needed to meet business and information protection objectives
    - coordinating information security and privacy activities throughout COMPANY
    - providing the appropriate tools and metrics to business management to properly measure the state of information security within COMPANY
    - meeting regularly with Senior Management
    - meeting on at least an annual basis with the Board of Directors
* **Information Security Organization** is responsible for evaluating, recommending, and instituting information security controls for business processes which handle and manage non-public information. In addition, the Information Security Organization (Operations, Engineering, and Architecture) is responsible for designing, building, implementing, and maintaining the Information Security Program. This includes:
  + - implementing information protection, privacy, and security relevant policies, standards, procedures, and guidelines
    - developing and maintaining information handling and protection guidelines
    - designing, implementing, and maintaining the corporate-wide security architecture
    - developing a formal inventory of systems and processes that involve transfer and protection of customer non-public information (including third parties)
    - developing and maintaining Information Security Awareness materials
    - monitoring vulnerability bulletins and defining processes to ensure identified vulnerabilities are evaluated and fixes are tested and implemented
    - developing and maintaining an incident response plan and procedures
    - developing an application development security certification process
    - collecting and maintaining security related metrics
    - performing and supervising security operations such as the monitoring of firewalls and intrusion detection systems, review of audit logs, and user and administrator account management
    - working with Internal Audit to perform annual assessments to applicable regulatory and legal information protection requirements
    - working with the Governance Team to validate compliance to Information Security Policies and Standards
* **Internal Audit** is responsible for validating compliance to Information Security Policies and Standards and regulatory compliance.
* **IT Governance Team** is responsible for validating compliance to Information Security Policies, Standards, Operating Procedures, and Configuration Guidelines.
* **Information Owner** is responsible for determining the value associated with potential loss or damage to business information assets. In addition, the information owner must determine and monitor access to business information assets. This access will be based upon user responsibilities. Additionally, the information owner must assign a classification designation to the asset and ensure the protection controls are equal to the level of classification assigned. The information owner must also ensure a risk assessment is completed on the asset.
* **Information Security Representative** within each COMPANY Entity and/or Business collecting is responsible for ensuring that the collection and management of the Non-Public Information is compliant with applicable COMPANY Data Privacy Policies and Operating Procedures.
* **Users** are responsible for safeguarding and monitoring COMPANY information assets against unauthorized disclosure, modification, and destruction. Users must follow password protection, access controls, and information handling security guidelines identified in the Information Security Policies and Standards at all times. Users should know, understand, and be held accountable for fulfilling their security responsibilities. Users are responsible for educating contractors, vendors, consultants, clients, and all other persons having access to COMPANY’s computing assets or information of their duties and restrictions.
* **Senior Management** is responsible for supporting and monitoring the effectiveness of and compliance with the Information Security Program and the Information Security Policies. This includes:
  + - clearly supporting all aspects of the Information Security Program
    - implementing the Information Security Program as approved by the Board of Directors
    - establishing appropriate policies, procedures, and controls
    - participating in assessing the effect of security issues on COMPANY and its business lines and processes,
    - working with Chief Information Security Officer in reviewing risk measurement definitions and criteria and acceptable levels of information security risks as outlined by the Chief Information Security Officer
    - delineating clear lines of responsibility and accountability for information security risk management decisions
* **Partners and Third Party Providers** are responsible for securing any business information assets to which they have access and ensuring no further dissemination of the information takes place to any other third party.
* **Board of Directors** is responsible for approving the Information Security Policies and to oversee management’s performance of its responsibilities as outlined in the Information Security Program. The Board’s oversight role requires it to review reports on the effectiveness of the Information Security Program. The Board has delegated to the Audit Committee its responsibilities under the Information Security Program. While the Board has the responsibilities and the powers set forth above, it is not the duty of the Board to prepare the Information Security Program, provide direct oversight of the program, or conduct audits of the program. This is the responsibility of management.
* **Audit Committee** is responsible for reviewing on an annual basis a report on the effectiveness of the firm’s Information Security Program. The annual report should describe the overall status of COMPANY’s Information Security Program. At a minimum, the report should address:
  + - the results of the risk assessment process
    - the results of management assessments and reviews
    - risk management and control decisions
    - service provider arrangements
    - results of security monitoring and testing
    - internal and external audit activity related to information security
    - third-party reviews of the information security program and information security measures
    - other internal or external reviews designed to assess the adequacy of the firm’s information security controls
    - security breaches or violations and management’s responses
    - recommendations for changes to the information security program