[INSERT FIRM LEGAL NAME]
Information Security Committee Charter

[Insert Firm Logo]

Version 1.0
[Insert Date]

This document and is proprietary and confidential. The document and information contained herein may not be shared outside of [Insert Firm Legal Name] unless approved by authorized personnel.

Need more help? Contact us at https://www.riskigy.com

Contents

Instructions

Documents are in a template format and are to be customized to fit the appropriate business and operational requirements. Use the sample as a foundation to build a bespoke policy for your business.

If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company specific document. **Otherwise, it would be a liability exposure to establish a policy and not to comply with it.**

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of the policy subject. Businesses should deploy a defense-in-depth security model of technical, operational, and physical security controls.

Delete the instructions after finalizing and adopting the policy.

Purpose

The mission of the Information Security Program is to protect the confidentiality, integrity and availability of Data.

- Confidentiality means that information is only accessible to authorized users.
- Integrity means safeguarding the accuracy and completeness of Data and processing methods.
- Availability means ensuring that authorized users have access to Data and associated Information Resources when required.

This Charter establishes the various functions within the Information Security Program and authorizes the persons described under each function to carry out the terms of the Information Security Policies.

- Coordinate the design and implementation of the Information Security Program.
- Document and communicate the status of the Information Security Program to the Management Team and Staff.
- Coordinate and sponsor interdepartmental projects related to the implementation of Information Security at the organization.
- Routine review Information Security Policies, Standards, and Processes & Procedures to ensure that they meet regulatory requirements, current standards and best practices.

- Approve changes to Information Security Standards and Processes & Procedures in order to comply with the organization's Policy, Regulatory and Compliance requirements.
- Sponsor and champion changes or updates to the Information Security Policy through the organization's approved processes.
- Review and approve exceptions to Information Security Policies, Standards, and Processes & Procedures.
- Ensure regulatory and routine required employee information security training is completed for their organizational hierarchy, role and responsibilities.

Membership

Committee Members are assigned by Senior Staff and represent the primary owners and stakeholders of Information Security at the organization.
Initial members have been identified as the following:

- Member 1
- Member 2
- Member 3
- Member 4

Compliance

Meetings:
The committee will meet at least every quarter (4 times a year) to review the state of information security, compliance, and planning purposes.

Exceptions

None

Definitions and Terms

None

Revision Table

Revision History				
#	**Version #**	**Date**	**Updates/Changes**	**Owner**
1	1.0	2022	Initial Draft	Riskigy
2				