Information Security Committee Charter

Introduction

Protection of the information entrusted to (District/Organization) by our stakeholders, employees, third-parties, and clients is important to the success of our organization. In an effort to design, implement, and manage an effective information security program, (District/Organization) has created the (District/Organization) Information Security Committee.

Purpose

The Information Security Committee exists to provide recommendations to (District/Organization) executive management in regard to all information security efforts undertaken by (District/Organization). The committee also coordinates and communicates the direction, current state, and oversight of the information security program.

Audience

The recommendations made, and actions taken by the (District/Organization) Information Security Committee may affect some or all (District/Organization) personnel, processes, and technologies.

Members

The members who participate in the (District/Organization) Information Security Committee are critical to the success of the (District/Organization) information security program. The (District/Organization) Information Security Committee is a cross-functional group comprised of employees representing different parts of the organization.

Responsibilities

The responsibilities of the (District/Organization) Information Security Committee are:

* Formulate, review, and recommend information security policy
* Review the effectiveness of policy implementation
* Provide clear direction and visible management support for security initiatives
* Initiate plans and programs to maintain information security awareness
* Ensure that security activities are executed in compliance with policy
* Identify and recommend how to handle non-compliance
* Approve methodologies and processes for information security
* Identify significant threat changes and vulnerabilities
* Assess the adequacy and coordinate the implementation of information security controls
* Promote information security education, training and awareness throughout (District/Organization)
* Evaluate information received from monitoring processes
* Review information security incident information and recommend follow-up actions
* Educate the team and staff on ongoing legal, regulatory and compliance changes as well as industry news and trends

Meetings

The (District/Organization) Information Security Committee will meet either in-person or through electronic means (teleconference, video conference, etc.) on a regular, periodic basis.

Decision Making

All decisions and recommendations made by the (District/Organization) Information Security Committee must be unanimous. In the event that a unanimous decision or recommendation cannot be attained, the committee will present the decision and/or recommendation to the President for intervention and final decision-making.

Agenda

An agenda should be prepared for each (District/Organization) Information Security Committee meeting. The agenda should be communicated to all committee members prior to the commencement of the meeting.

Attendance

Members of the (District/Organization) Information Security Committee are strongly encouraged to participate in all committee activities and attend all committee meetings. In the event that a member cannot attend a meeting, the member should communicate his/her responses to the agenda items and/or send a delegate attendee with the authority to speak for the committee member.

Communication

(District/Organization) Information Security activities, recommendations, and decisions must be documented and available to appropriate personnel.

Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version  | Modified Date | Approved Date | Author | Reason/Comments |
| 1.0.0 | August 2016 |  | SecurityStudio | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |