Information Security Program Overview

An introduction to information security program creation and maintenance

Introduction

(District/Organization) is making a demonstrated commitment to improve information security throughout the organization. To this end, (District/Organization) is in process of developing several information security policies that will form the governance and foundation for the (District/Organization) Information Security Program (\*see Appendix for a preliminary list of polices to be developed). For the information security policies to provide value they must be approved by management and adopted throughout the organization. To ensure that all aspects of Information Security are covered in the new Information Security Program, the program will be based on the international standard for Information Security Code of Practice for Information Security Management (ISO/IEC 27002:2013).

This document provides a conceptual plan towards adoption and full implementation, and some general guidance regarding what works and what does not. The plan is based on experiences with hundreds of other organizations across a spectrum of sizes and industries.

Purpose

### (District/Organization) Information Security Program

There are multiple reasons or purposes for the (District/Organization) Information Security Program:

* Ensure that appropriate measures are taken to protect the confidentiality, integrity, and availability of information entrusted to the organization by its customers, business partners, and stakeholders.
* Provide management with assurance that the organization is doing what it should with respect to information security.
* Provide customers, business partners, and stakeholders with assurance that (District/Organization) is protecting their information.
* Assist in compliance with regulatory requirements; current and expected.

Information Security Program Lifecycle

The (District/Organization) Information Security Program will be based on sound risk management principles and a lifecycle of continuous improvement as depicted in the (District/Organization) Security Program Lifecycle in Fig.1.



**Figure1: (District/Organization) Information Security Program Lifecycle.**

Develop to Approve

At this point in the lifecycle, (District/Organization) is planning what policies are needed and what they must contain. Once the policies are finished being developed they will move on for approval by the board of directors. The policy approval process is depicted in Figure 2.

###

**Figure 2: (District/Organization) Information Security Policy Approval Process.**

There are three steps to security policy approval. First, the policies are drafted by the Information Security Working Group. Next, the draft policies are reviewed, commented on, and edited by the Information Security Committee. The final step is submitting the published policy documents to the Board of Directors for formal approval.

Approve to Adopt

At this point in the lifecycle, (District/Organization) is planning how best to adopt the policies that have been developed and are subject to approval.



There are five steps that are essential for (District/Organization) to move to adoption of the Information Security Program; Communication Plan, Supporting Documentation, Assess Gaps, Develop Plans, and Implement.

Communication Plan Development

Perhaps the most important first step in moving from approval of information security policies to adoption of security policies is the determination and planning for how (District/Organization) is going to best communicate to management, employees, contractors, and others.

The communication plan will help us to ensure that we communicate with the organization consistently, effectively, regularly, and as transparently as possible. The plan lays out who we communicate with, when we must communicate, what we must communicate, and how we must communicate.

The communication plan is a live document that changes with the organization; in developing the communication plan, we will need to identify methods for which we will measure its effectiveness.



Announcement

The redevelopment and implementation of a new (District/Organization) Information Security Program is a new initiative for the organization; making an appropriate and effective announcement is important.

Training

Expecting people to follow the direction provided by the (District/Organization) policies without proper training is bound to fail. Effective information security training is fresh, relevant, and develops a sense of ownership among the (District/Organization) community.

Awareness

Information security is not closely integrated with the (District/Organization) culture today. Ongoing awareness campaigns are used as a method of reminding people of their role in protecting sensitive information and keeping people up-to-date on information security news. Awareness campaigns can (and should) be fun and interactive.

Notifications

Changes to processes and technologies that affect people must be communicated to people. Often people are fine with change, as long as they understand the need for change. In general, any change made to any (District/Organization) process or technology must be communicated to all of the people affected by the change, before, during, and after the change.

(District/Organization) management needs to be notified regularly and kept up-to-date on significant events.

Feedback

The (District/Organization) Information Security Program is not any one person’s responsibility, and it is not “owned” by any one person. The (District/Organization) Information Security Program is everybody’s responsibility and it is “owned” by everyone. We need to encourage people to participate, and their feedback is critical to our success.

Feedback must be sought and received from [Company Address] management regularly.

Develop Supporting Documentation

Policies provide the governance and direction for the (District/Organization) Information Security Program, supporting documents provide the details for how to comply with policies.



Guidelines

(District/Organization) guidelines provide directions to comply with policy that are not mandatory. Guidelines provide “guidance”. Guidelines may apply to all persons, certain persons within a specific department, or individuals across departments. Most guidelines are developed by information technology personnel.

Standards

(District/Organization) standards provide mandatory directions and/or boundaries for policy compliance. Specific technical details may be included in certain standards. Standards may apply to all persons, certain persons within a specific department, or individuals across departments. Most standards are developed by information technology personnel.

Procedures

Procedures provide step-by-step directions to complete certain tasks. Procedures are mandatory. Procedures may apply to all persons, certain persons within a specific department, or individuals across departments. Procedures are developed by anyone that has a need to carry out a task in a repeatable and efficient manner.

Assess Compliance Gaps

There are many places within (District/Organization) where there may be non-compliance with sound information security principles and stated policy. At this step of the adoption, the policies are reviewed in detail with the focus on identifying individual policy statements for which (District/Organization) is not compliant. The non-compliant policy statements are put into context and perspective at the Develop Plans stage of adoption.

Develop Plans

The non-compliant policy statements are organized into categories and prioritized. Plans and projects are developed, resources identified, and timelines established.

It is important to develop projects and plans that are most efficient; for example, a single project that addresses dozens of non-compliant policy statements is much more efficient than multiple projects that address a few non-compliant policy statements.

Each project plan must be accompanied with a notification plan that fits with the original communication plan (covered above).

Implement

The last stage in the adoption of the (District/Organization) information security policies is implementation. Implementation consists of execution and documentation of the projects that were developed in the previous stage (Develop Plans) of adoption. At the end of implementation of controls or processes, documentation should be prepared to ensure the ongoing management of the controls or processes remains in compliance with stated policy objectives.



**Figure1: (District/Organization) Information Security Program Lifecycle.**

Adopt to Manage

At this point in the lifecycle, (District/Organization) is to manage and reinforce compliance of the information security policies that were implemented during the adoption phase of the lifecycle. Management of the program may include but not limited to reviewing audit results, logs, holding the security committee meetings that are noted in policy, etc.

Manage to Assess

At the Assess phase of the lifecycle, the (District/Organization) information security program is reviewed to verify if the policies are still relevant or need to be updated. Policies should be assessed or reviewed at least annually or when a significant event causes the need for a change to policy.

Questions

Questions regarding this plan can be directed to:

Information Security Committee

# Appendix: (District/Organization) Policy Checklist

The following checklist contains policies that should\* be created to establish a functional and effective information security governing framework for (District/Organization).

*\*Based upon experience with similar organizations and the results of the administrative controls review conducted (District/Organization).*

### Policy Checklist

Some of the policies mentioned in this list may include re-writes or modifications to existing documentation as opposed to new policies.

[ ] Information Security Policy

[ ] Acceptable Use Policy

 [ ] Asset Management Policy

[ ] Audit Policy

[ ] Change Control Policy

[ ] Disaster Recovery Policy

[ ] Encryption Management Policy

[ ] Identity and Access Management Policy

[ ] Incident Management Policy

[ ] Information Classification and Management Policy

 [ ] Network Management Policy

[ ] Personnel Security Policy

[ ] Physical Security Policy

[ ] Risk Management Policy

[ ] Security Training and Awareness Policy

[ ] System Development and Acceptance Policy

[ ] Vendor Management Policy

[ ] Vulnerability Management Policy