

Information Security Program (ISP) Implementation Guidelines

# Purpose

**<Utility Name>** recognizes the need to involve all employees to effectively implement the Information Security Program (ISP).

*[Explanatory Note: This policy draft is intended for establishing a process for implementing an ISP at the Board of Directors (BOD) level with policies and procedures which the staff will implement and follow. Examples of organizational hierarchy most likely will require modification to reflect organizational structure of a particular Utility.]*

# Scope

This document provides guidelines for the effective implementation of an Information Security Program (ISP), and will emphasize the importance of defining document types and a model for assigning responsibility. The scope of the ISP is broader than the IT discipline. These guidelines suggest establishing a Steering Committee to develop a security-conscious culture throughout the organization.

# Guidelines

## Documents structure

The ISP will use the following documentation structure:

* + 1. Policy

A Policy is a formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area. Policies always state required actions, and may include pointers to standards. Policy attributes include the following:

* Require compliance (mandatory)
* Failure to comply results in disciplinary action
* Focus on desired results, not on means of implementation
* Further defined by standards and guidelines
  + 1. Standard

A Standard is a mandatory action or rule designed to support and conform to a policy.

* A standard should make a policy more meaningful and effective
* A standard must include one or more accepted specifications for documentation, hardware, software, and behavior
  + 1. Procedure

A Procedure describes the process of implementing a Policy and enforces that Policy. A Procedure is a series of steps taken to accomplish an end goal:

* Defines "how" to protect resources and are the mechanisms to enforce policy
* Provides a quick reference in times of crisis
* Eliminates the problem of a single point of failure; and
* Also is known as a Standard Operating Procedure (SOP)
  + 1. Guidelines

General statements, recommendations, or administrative instructions designed to achieve the policy's objectives by providing a framework within which to implement procedures.

* A guideline can change frequently based on the environment, and should be reviewed more frequently than standards and policies
* A guideline is not mandatory, rather a suggestion of a best practice. Hence "guidelines" and "best practices" are interchangeable
  + 1. Forms and other documents

Forms are used to create records, checklists, surveys, or other documentation used in the creation of a product or service. Records are a critical output of any procedure or work instruction and form the basis of process communication, audit material, and process improvement initiatives.

## Responsibility model

The Information Security Program uses the RACI model for assigning responsibility during its implementation. The RACI model is a common project management tool. The acronym RACI stands for:  
  
**R** – **Responsible** – (also ***Recommender***)   
Those who do the work to achieve the task. There is at least one role with a participation type of *Responsible*, although others can be delegated to assist in the work required.

**A** – **Accountable** – (also ***Approver*** or *final approving authority*)  
The one ultimately answerable for the correct and thorough completion of the deliverable or task, and the one who delegates the work to those *Responsible*. In other words, an *Accountable* must sign off (approve) work that *Responsible* provides. There **must** be only one *Accountable* specified for each task or deliverable.

**C** – **Consulted** (sometimes ***Consultant*** or *counsel*)  
Those whose opinions are sought, typically [subject matter experts](https://en.wikipedia.org/wiki/Subject_matter_expert) and with whom there is two-way communication (in other words, the *Consulted* contributes to the task or deliverable, providing input and suggested output).

**I** – **Informed** (also *Informee*)  
Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication (as receivers to information).

## Implementation Process

* BOD approves Information Security Policy and ISP Implementation Guidelines
* CEO establishes Information Security Policy Steering Committee (ISSC)
* ISSC shall include staff from Administration, IT, E&O, Accounting, HR, Legal, etc.
* ISSC responsibilities include:
  + - Coordinate initial assets inventory and data classification  
      ISPL includes *Data Classification Policy* and *Data Assets Inventory Form*
    - Coordinate risk assessment  
      ISPL *Risk Assessment Procedure* and *Risk Register Form* can be used to support risk assessment.
    - Coordinate gap analysis  
      PCI DSS (Payment Card Industry Data Security Standard) or DOE C2M2 (Cyber can be used for gap analysis which can be conducted internally or by external consultant.
    - Meeting on regular basis and use project management tools to plan, monitor and control implementation process
    - Selecting policies and standards for implementation
    - Using RACI model for assigning responsibilities for implementing each policy and standard
    - Review and recommend changes to existing policies, procedures, standards and forms

# Related Standards, Policies, and Processes

* Inspired by “Cyber Security Policy Framework”   
  (<https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx>)   
  The Cyber Security Policy Framework was created by the Kentucky Association of Electric Cooperatives (KAEC) Information Technology (IT) Association - Cyber Security Subcommittee.

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| CEO/GM | **BOD** | **Legal Department** | **All Employees** |

*[Explanatory Note: Utility should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |