# Information Security Program Plan (ISPP)

| | |
|---|---|
| ***Official Policy Title:*** | |
| ***Responsible Party:*** | |
| ***Approval Party:*** | |
| ***Effective Date:*** | |
| ***Last Update:*** | |
| ***Version Number:*** | |
| ***Policy Framework:*** | **Developed in accordance with NIST Special Publication (SP) 800 Series - https://csrc.nist.gov/publications/sp800** |
| ***Mapping*** | **(1). NIST SP 800-53, rev. 5 (PM-1).** |

## Overview

An Information Security Program Plan (ISPP) [the "plan"] is a formal document that provides an overview of the security requirements of an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. As such, the following information details [company name]'s ISPP as required by the National Institute of Standards and Technology.

Additionally, an ISPP documents an organization's implementation details regarding the relevant program management and common controls. As such, the plan is to provide sufficient information about the controls to enable implementations that are unambiguously compliant with the intent

of the plan and a determination of the risk to be incurred if the plan is implemented as intended. Updates to the ISPP are to include organizational changes and problems identified during plan implementation or control assessments.

Program management controls may be implemented at the organization level or the mission or business process level and are essential for managing the organization's information security program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular system. Together, the applicable individual system security plans and the organization-wide information security program plan for [company name] are to provide complete coverage for the security controls employed within the organization.

Common controls available for inheritance by organizational systems are to be documented in an appendix (Appendix A) to the organization's ISPP unless *the controls are included in a separate security plan for a system*. The ISPP is to indicate which separate security plans contain descriptions of common controls. Events that may precipitate an update to the ISPP include, but are not limited to, organization-wide assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines.

**Note:** Common controls are security controls that can support multiple information systems efficiently and effectively as a common capability. When these controls are used to support a specific information system, they are referenced by that specific system as inherited controls.

Many of the security controls needed to protect organizational information systems (e.g., contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls) are excellent candidates for common control status. Information security program management controls within this stated ISPP document may also be deemed common controls by the organization since the controls are employed at the organizational level and typically serve multiple information systems.

## Introduction

The ISPP referenced within this document defines the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, the ISPP is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The ISPP is to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

## Purpose

The purpose of the ISPP is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component.*

- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

## Scope

The ISPP encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is described as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

**Requirements for the Security Program** [NIST PM-1(a)1]

As documented in the organization's System Security Plan (SSP), along with this document herein, the requirements for the security program are to ensure the Confidentiality, Integrity, and Availability (CIA) of [company name]'s information systems, thus, allowing for the expected delivery of services and solutions as designed by the information systems. Specifically, [company name]'s information systems are to ensure the following:

- Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity — guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.

- Availability – ensuring timely and reliable access to and use of information.

Additionally, the requirements for the security program are to ensure that all in-scope NIST SP 800 control families have appropriate technical, security, and operational controls in place for helping ensure the CIA of [company name] information systems. Protecting organizational assets by implementing policies, procedures, and processes consistent with the CIA triad requires a concerted effort and collaboration by all personnel throughout the organization.

**Identification and Assignment of Organizational Roles and Responsibilities** [NIST PM-1(a)2]

The following personnel constitute the organization's commitment to the ISPP. Specifically, such personnel are instrumental in executing their daily roles and responsibilities for helping ensure the CIA of [company name] information systems.

| Title | Name | Contact Information | ISPP Roles & Responsibilities | Coordination Roles with Other Internal Entities | Additional Notes and Comments |
|---|---|---|---|---|---|
| **Chief Executive Officer (CEO)** | | | | | |
| **President** | | | | | |
| **Chief Technology Officer** | | | | | |
| **Chief Information Officer** | | | | | |
| **Chief Security Officer** | | | | | |
| **Network Engineer - Internal** | | | | | |
| **System Administrator - Internal** | | | | | |
| **Customer Support Representatives (CSR) - Internal** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **Database Administrator (DBA) - Internal** | | | | | |
| **Software Developers – Internal** | | | | | |
| **End-User of Systems (Clients)** | | | | | |
| **Please add more users** | | | | | |
| **Please add more users** | | | | | |
| **Please add more users** | | | | | |

**Coordination among Organizational Entities for Information Security** [NIST PM-1(a)3]

A designated senior information security officer is to ensure that all aspects of information security for the information systems are appropriately coordinated with all respective company-wide divisions and departments. This requires constant communication and an open dialogue amongst personnel to help facilitate a security-first mindset for the entire organization, one that advocates the CIA triad at all times. Additionally, the senior information security officer is to undertake the following measures for ensuring coordination with all respective company-wide divisions and departments:

- Regularly communicate and discuss information security issues, making program adjustments as necessary.
- Collaborate on continuing information security best practices, including discussions on how to continue to improve the organization's overall security and privacy initiatives.
- Engage and participate in all aspects of information security plan and program development, testing exercises, and continuous monitoring.
- Report regularly upstream to senior management on the status of the ISPP and all other company-wide related information security initiatives.

**Information Security Program Leadership Role** [NIST PM-1(a)4] and [NIST PM-2]

[Company name] is to appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

| Name of Senior Information Security Officer | Title | Roles and Responsibilities |
|---|---|---|
| | | Responsible for coordinating, developing, implementing, and maintaining the organizational-wide Information Security Program Plan (ISPP). |

Additionally, the senior information security officer has the following roles and responsibilities:

- Coordinate the continuous development, implementation and updating of security and privacy policies, standards, guidelines, baselines, processes, and procedures as necessary.
- Develop and manage the frameworks, processes, and tools necessary for IT to properly manage risk and to make risk-based decisions related to IT activities.
- Proactive identification and mitigation of IT risks as well as responding to observations identified by third party auditors or examiners as necessary.
- Assist in all necessary remediation efforts.
- Ensure overall IT compliance with regulatory requirements through proactive planning and communication, ownership, and relationships.
- Identify acceptable levels of residual risk and assist with action plans, policy, and procedural changes for risk mitigation.
- Provide strategic recommendations to key IT projects to help improve project results, quality of deliverables, risk optimization, security processes and compliance with regulations.
- Respond accordingly to allegations of security incidents and conduct investigations as necessary, along with preparing written findings, recommendations and follow up evaluation.
- Work as an appropriate liaison with local, state, and federal authorities requiring information and reports on security incidents to include campus police, FBI or other law enforcement agencies.

Note: For purposes of the ISPP, the senior agency information security officer is an organizational official. Additionally, [Company name] may refer to this official as the senior information security officer or chief information security officer, or a related title that is similar.

**Review and Update of ISPP** [NIST PM-1b]

[Company name] is to update the ISPP at a minimum, annually, or sooner, when the following conditions or events warrant such:

- Material changes to the information systems, specifically, changes in the architecture to include removing or adding assets into the network.
- Organizational changes in key leadership positions for which personnel have specific ISPP roles and responsibilities.
- Any other events that have the ability to impact the overall intent and rigor of the content of the ISPP.

**Protection of Plan** [NIST PM-1c]

Only authorized personnel - those with a need-to-know right - are to be granted access to the ISPP. The ISPP is to be distributed electronically via pdf format to such personnel, with no editing rights allowed. Furthermore, the ISPP is not allowed to be sent either hard-copy or electronically to any external, third-party, unless approval has been granted by authorized personnel within [company name].

**Information Security and Privacy Resources** [NIST PM-3]

Both information security and privacy are two critically important issues that must be continuously addressed for ensuring the safety and security of [company name]'s assets. As such, authorized personnel are to champion all necessary InfoSec and privacy measures for the organization, which entails the following:

- Assess and request all necessary resources from senior leadership.
- Prepare all necessary documentation (i.e., budgets, technology, and H.R. requests, etc.) for senior leadership.
- Regular review of all necessary resources and reporting upstream to senior leadership of the status of such measures.

**Plan of Action and Milestones** [NIST PM-4]

[Company name] is to implement a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are reported in accordance with OMB FISMA reporting requirements, and to review plans of action and milestones for the security program and associated organization information systems for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

**Personnel responsible for POAM measures include the following:**

| Name | Title | Responsibilities | Contact Information |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**System Inventory** [NIST PM-5]

[Company name] is to develop and maintain an inventory of its information systems. Additionally, if [company name] stores, processes, and/or transmits Personally Identifiable Information (PII), an inventory of the PII is to be established, maintained, and updated [define frequency of updating the PII inventory]. System inventory measures consist of the following: [Discuss system inventory measures].

**Measures of Performance** [NIST PM-6]

[Company name] is to monitor the results of information security measures of performance. As such, the results are to be provided as part of the organization's Continuous Monitoring Program. [Note: If you do NOT have such a program in place, please visit the Arlington Security Portal (ASP), where you can purchase and immediately download the program].

## Enterprise Architecture [NIST PM-7]

[Company name] is to develop and maintain an enterprise architecture with consideration for information security, privacy, and other related measures. Specifically, such an architecture is to be designed, developed, implemented, and maintained by employing Defense-in-Depth and Layered security - essentially utilizing various resources for helping protect one's network. Defense-in- Depth – for purposes of information security – includes the following layers, which have been loosely adopted and agreed upon by industry leading vendors and other noted organizations:

- Data
- Application
- Host
- Internal Network
- Perimeter
- Physical
- Policies, Procedures, Awareness

Layered security, often mentioned in the context of Defense-in-Depth, is a concept whereby multiple layers of security initiatives are deployed for the purposes of protecting an organization's critical information systems. Specifically, by utilizing several security tools, protocols, and features, organizations can effectively put in place layers of security that – in the aggregate – help ensure the confidentiality, integrity, and availability (CIA) of systems.

## Critical Infrastructure Plan [NIST PM-8]

For helping address information security risks, [company name] is to regularly assess The National Infrastructure Protection Plan (NIPP)—NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. Specifically, NIPP 2013 outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.

NIPP 2013 meets the requirements of Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience, signed in February 2013. The Plan was developed through a collaborative process involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry. It provides a clear call to action to leverage partnerships, innovate for risk management, and focus on

outcomes. As such, specific documentation for which [company name] regularly assesses consists of the following (located at https://www.cisa.gov/national-infrastructure-protection-plan)

- NIPP 2013 Supplements
- 2017 NIPP Security and Resilience Challenge
- Sector-Specific Plans
- More on the National Infrastructure Protection Plan
- Training Courses
- Authorities

**Risk Management Strategy** [NIST PM-9]

[Company name] is to develop a comprehensive strategy to manage security risks to organizational operations and assets, individuals, other organizations, and the nation associated with the operation and use of organizational systems; and privacy risk to individuals resulting from the authorized processing of personally identifiable information; implement the risk management strategy consistently across the organization; and review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.

Currently, [company name]'s risk management strategies, which are documented in the [name of risk management policy/procedures/program document] and consist of the following measures: [Note: If you do NOT have such a program in place, please visit the Arlington Security Portal (ASP), where you can purchase and immediately download the 'Risk Management Strategy Program' template].

- Performing a risk assessment annually, at a minimum, and more frequently if circumstances warrant.
- Reporting upstream to senior management the results of the risk assessment, specifically, the findings, and relevant recommendations to take for reducing risk exposure.
- Coordinating with appropriate personnel in performing necessary tasks to correct issues and concerns identified during the risk assessment process.

**Authorization Process** [NIST PM-10]

[Company name] is to manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes and to also designate individuals to fulfill specific roles and responsibilities within the organizational risk management process, along with integrating the authorization processes into an organization-wide risk management program.

**Personnel responsible for Authorization Processes for [company name] Information Systems**

| Name | Title | Responsibilities | Contact Information |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Mission and Business Process Definition** [NIST PM-11]

[Company name] is to define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the nation; and determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and to review and revise the mission and business processes as necessary. Specifically, this requires the following:

Defining Organizational and Mission Business Processes: Authorized personnel are to ensure that a strategic alignment exists in terms of defining organizational and mission business processes with that of information security and privacy issues and risks. Ensuring the CIA of [company name] assets requires implementing all necessary information security and cybersecurity measures, along with data privacy measures for ensuring the safety and security of organizational data, including Personally Identifiable Information (PII).

Determine Information Protection and PII Processing Needs: Data that is stored, processed, and transmitted by [company name] must be protected at all times. As such, authorized personnel are to undertake all necessary data mapping measures for determining the types of data resident in [company name]'s systems, its purpose and use, and the relevant protection measures in place for ensuring the safety and security of such data.

Review and Revision of Mission and Business Processes: It is the policy of [company name] to review, and revise, as necessary, all mission and business processes annually, at a minimum, and more frequently if circumstances warrant such.

**Insider Threat Program** [NIST PM-12]

[Company name] is to Implement an insider threat program that includes a cross-discipline insider threat incident handling team. [Company name] has in place an insider threat program, with the specifics of the program noted below: [Note: If you do NOT have such a program in place, please visit the Arlington Security Portal (ASP), where you can purchase and immediately download the 'Insider Threat Program' template].

Insider Threat Program Information

| Name of Program | Details of the Program | Program Owner(s) | Implementation Measures for the Program |
|---|---|---|---|
| | | (1).<br>(2).<br>(3). | |