Template: Master Information Security Policy & Procedures (MISPP)

Draft v3

21 Sep 2020

Distribution: **Public**

The following material is a master information security / cybersecurity policy template designed to represent the most central governing policies for an organization's cybersecurity program. including programmatic commitments, roles and responsibilities; references to other special purpose policies. As such, it represents "the Constitution" of the cybersecurity program.

This new draft version is updated to align to the Trusted CI Framework, as well as include improved default guidance on what to consider including. Guidance or placeholders for organizations using this template are blue and in brackets [like this]. Normal black text is example language. We strongly encourage organizations using this template to tailor the content and structure.

We anticipate updating this template to a finalized v3 in early CY2021.

Master Information Security Policy & Procedures

[Organization Name]

[Version Number]
[Date of Publication]

[Description of intended audience or scope of authorized distribution]

Authors: [Names and roles]
Chief Information Security Officer: [Name, and role-based contact information (e.g., ciso@organization.org)]
Approved by: [Name, Role]

Table of Contents

1 Purpose, Scope, and Applicability

[Describe the purpose, scope, and applicability of this policy. Include a cybersecurity program's mission and how it relates to the organization's mission(s). If the organization is a unit of a parent organization, describe the nature of the relationship for cybersecurity purposes.]

This document represents the core cybersecurity / information security policies for [ORGANIZATION NAME], including programmatic commitments, roles and responsibilities; references to other special purpose policies. "Cybersecurity" is defined in Appendix B, and is used interchangeably with "information security" in this policy and for the purposes of the cybersecurity program.

The policy applies to all [ORGANIZATION NAME] personnel and units.

2 Programmatics

This section describes policy and procedures that govern our cybersecurity program. For more information on the cybersecurity program. General information about the program can be found at [insert URL].

2.1 Framework

[Describe any program or process frameworks the organization has adopted as a basis for the cybersecurity program. Provide a reference, pointer, or contact role to learn more about any third party obligations that have driven framework adoption decisions.]

[ORGANIZATION NAME]'s cybersecurity program is based on the Trusted CI Framework (trustedci.org/framework).

2.2 Baseline Control Set

[Describe the default baseline control set the organization has adopted. Provide a reference, pointer, or contact role to learn more about any third party obligations that have driven control set adoption decisions.]

[ORGANIZATION NAME] has adopted the CIS Controls v7.1 as our baseline control set. Specific details regarding the status and application of these controls can be found by [describe location or role].

2.3 Policy Development, Adoption, and Education

[Describe how cybersecurity policies are developed, adopted, disseminated and trained. Describe where stakeholders can find other cybersecurity policies, either referencing Appendix A or another authoritative source.]

2.4 Policy Enforcement

[Describe the means of enforcement and potential consequences of violations.]

Violations of [ORGANIZATION NAME] cybersecurity policies can result in loss of access to resources and services, and/or disciplinary action. Activities in violation of any laws may be reported to the law enforcement authorities for investigation and prosecution. Anyone who believes that there is a violation of a cybersecurity policy or has a related question should contact: [support email and/or phone number].

2.5 Policy Exceptions

[Provide contact information and describe the process for requesting and processing policy exception requests.]

2.6 Programmatic Evaluation

[Describe the frequency and general nature of evaluations of this policy and the cybersecurity program. Include information regarding how stakeholders can contribute.]

3 Roles & Responsibilities

[Explicitly describe roles and responsibilities of all organizational personnel (or classes of personnel) and any organizations or units with special cybersecurity responsibilities. This should include all roles and organizational entities with access to, control over, or authority over information assets (i.e., information systems, information/data). Explicitly describe responsibilities for cybersecurity decision making (e.g., what roles are authorized to accept cybersecurity risk on behalf of the organization) and communication.]

3.1 Senior Leadership

[Describe the role of senior organizational leadership in cybersecurity decision making and communications.]

[Insert senior leadership role] retains responsibility for cybersecurity risk acceptance except where expressly delegated in this policy or other governing documents.

3.2 Chief Information Security Officer

[Describe the CISO or equivalent role. Provide contact information to reach the CISO or cybersecurity team.]

[ORGANIZATION NAME] maintains a position of Chief Information Security Officer (CISO), who reports to [insert role, *e.g.*, the Director]. [Insert or reference the artifact that defines CISO's duties.]

3.3 All Organizational Personnel

[Describe the responsibilities that apply to all organizational personnel.]

All [ORGANIZATION NAME] personnel are responsible for reviewing and respecting cybersecurity policies and procedures, including this one.

Each staff member is expected immediately to report any known or suspected violations of security policies or procedures, or known or suspected cybersecurity incidents to the CISO or senior leadership.

3.4 Third Parties

[List or provide a reference to policies and procedures that apply to third parties (e.g., collaborators, resource users, contractors, visitors) including where they are located and/or how users access them. These may include Terms of Service, Acceptable Use Policies, Privacy Policies]

Third parties are responsible for reviewing and respecting the following policies while accessing or using [ORGANIZATION NAME] resources. Cybersecurity-related external user policies include:

Appendix A: Other Policy and Procedure Documents

[Unless directing stakeholders to another location to find other cybersecurity policies and procedures, use this Appendix to provide a guide. Include all other active special purpose cybersecurity policy documents, including their locations and version numbers and/or dates of publication, so this master document remains an authoritative list of active policies and procedures. The following is a non-exclusive list of other documents you may need.]

In addition to this Master document, [ORGANIZATION NAME] has adopted the following additional policies and procedures.

- Acceptable Use Policy - Set of rules that a user must agree to follow in order to be provided with access to a network and/or resources. Used to reduce liability and act as a reference for enforcement of policy.
- Access Control Policy - Defines the resources being protected and the rules that control access to them.
- Adjunct, Subawardee, Subcontractor Policy - An agreement containing a set of rules and expectations to be used between two parties seeking access to the other's network, data or resources.
- Asset Management Policy - Requirements for managing capital equipment including: inventory, licensing information, maintenance, and protection of hardware and software assets
- Information Classification Policy - Used to ensure consistency in classification and protection of data.
- Disaster Recovery Policy - Contains policies and procedures for dealing with various types of disasters that can affect the organization.
- Personnel Onboarding Checklist - Form to be completed at the beginning of employment that addresses authorizing access to resources, physical space and any organizational assets checked out such as laptops.
- Personnel Exit Checklist - Form to be completed at the end of employment that addresses revoking access to resources, physical space and the return of organizational assets.
- Incident Response Procedures - A pre-defined organized approach to addressing and managing a security incident.
- Mobile Computing Policy - Establish standards for the use of mobile computing and storage devices.
- Network Security Policy - Outlines the rules for network access, determines how policies are enforced and lays out some of the basic architecture of the company security/ network security environment.
- Password Policy - A set of rules designed to establish security requirements for passwords and password management.
- Physical [and Environmental] Security Policy - Details measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.

- Privacy Policy - A statement that discloses the ways a party gathers, uses, discloses and manages a customer or client's data.
- Remote Access Policy - Outlines and defines acceptable methods of remotely connecting to the internal network.
- Training and Awareness Policy - Outlines an organization's strategy for educating employees and communicating policies and procedures for working with information technology (IT).

Appendix B: Terms and Acronyms

[Use this as a central location to define terms and acronyms for all information security policies.]

Cybersecurity: "prevention of damage to, protection of, and restoration of computers, electronic communication systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation."[1] This definition is scoped to include information assets beyond traditional IT, and includes operational technology.[2]

***

[1] https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

[2] "Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events." *See* https://www.gartner.com/en/information-technology/glossary/operational-technology-ot