Master Information Security Policy & Procedures

[Organization / Project Name]

[Version Number / Date of Publication]

[Insert description of intended audience or scope of authorized distribution.]

Authors: [Names]
Information Security Officer: [Name]

Table of Contents

1 Introduction
2 Roles & Responsibilities
  2.1 Management / Leadership
  2.2 Information Security Officer
  2.3 Project Personnel and Staff
  2.4 External Users
3 Developing, Implementing, and Maintaining Our Cybersecurity Program
  3.1 Information Security Risk Management Processes
  3.2 Enforcement
  3.3 Modifications to Information Security Policies and Procedures
4 Resources & Key Contacts
5 Other Policy and Procedure Documents
6 Terms and Acronyms

1 Introduction

This document represents the core information security policies and procedures for [ORGANIZATION/PROJECT NAME], including information security-related roles and responsibilities; references to other, special purpose policies; and the core procedures for developing, implementing, and maintaining the information security program.

Our information security program is a structured approach to develop, implement, and maintain an organizational environment conducive to appropriate information security and levels of information-related risk. This program entails ongoing activities to address relevant policies and procedures; technology and mitigations; and training and awareness.

2 Roles & Responsibilities

2.1 Management / Leadership

[If the Information Security Officer will be someone other than person or persons with ultimate management responsibility for the project/organization, consider including this section to describe the roles and responsibilities of project leadership in developing and supporting the information security program and formal relationship to the Information Security Officer.]

2.2 Information Security Officer

[ORGANIZATION/PROJECT NAME] maintains a position of Information Security Officer (ISO), who reports to [Project PI, CIO, Center Director]. The ISO has responsibility for overseeing and coordinating the components of the information security program. The ISO maintains all operative policy and procedure documents, including this document, will distribute them as appropriate. All reviews of [ORGANIZATION/PROJECT NAME] wide policies and procedures are coordinated and archived through this office. The ISO also documents any changes made to the security policy based on these reviews.

The ISO is the first point of contact for any request for clarification of [ORGANIZATION/PROJECT NAME] information security policy and procedures. The ISO will coordinates information security incident response, including correspondence between the affected staff and users.

As fo the date of publication of this document, the Information Security Officer is [NAME]. Contact information for the ISO follows:

[Insert all relevant contact information for the ISO.]

2.3 Project Personnel and Staff

It is the responsibility of each individual working for [ORGANIZATION/PROJECT NAME] to review and respect these policies and procedures. It is also the staff member's responsibility to understand the underlying policies that drive those detailed procedures, so that the individual is able to make rational decisions in situations not specifically covered by the detailed procedures.

Each staff member is expected immediately to report any known or suspected violations of security procedures, or known or suspected information security incidents to the ISO or project leadership. In all cases, the staff member and the time of the incident will be documented in order to support a timely analysis of and coordinated response to the situation.

2.4 External Users

External users are responsible for reviewing and respecting the following policies while using [ORGANIZATION/PROJECT NAME] resources. Information security-related external user policies include:

- [List all that apply (Acceptable Use Policy, Privacy Policy), including where they are located and/or how users access them]

3 Developing, Implementing, and Maintaining Our Cybersecurity Program

3.1 Information Security Risk Management Processes

[Include (a) a brief description of the risk management processes your project/organization has adopted and apply to information security; (b) references to any relevant resources, agreements, regulations, or other external information security requirements; (c) information regarding the repeated and/or continuous processes for assessing the cybersecurity program as a whole.]

3.2 Enforcement

Violations of [ORGANIZATION/PROJECT NAME] information security 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 proper authorities for investigation and prosecution. Anyone who believes that there is a violation of any information security policy or has a related question should contact: [support email or phone number].

3.3 Modifications to Information Security Policies and Procedures

The Information Security Officer (ISO) is responsible for coordinating changes to established policies and procedures. Requests for changes to established procedures should be presented to the ISO who will analyze the feasibility and the cost of changing the procedure. The ISO will

also collaborate with the staff responsible for implementing the recommended change before making a decision. The ISO approves all internal changes to policies and procedures.

[Insert information regarding how policy/procedure changes are published in your organization, and how those bound by the policies will be notified of the same.]

4 Resources & Key Contacts

[If relevant, include key references to information security resources and useful contact information, for example, to the campus information security office or law enforcement.]

5 Other Policy and Procedure Documents

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

[Include all other active special purpose information security 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. The Guide and provided templates and examples will help you select and develop your own policies.]

- 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 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).

6 Terms and Acronyms

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

***