Insert Logo Here

Organization Name

Security Policy

System & Communications Protection

Version 1.0

April 6, 2021

Proprietary and Confidential

For Authorized Use Only

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 4/6/2021 | 1.0 | Published SC Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68595138)

[2 Purpose 1](#_Toc68595139)

[3 Scope 1](#_Toc68595140)

[4 Roles and Responsibilities 1](#_Toc68595141)

[5 Management Commitment 2](#_Toc68595142)

[6 Authority 3](#_Toc68595143)

[7 Compliance 3](#_Toc68595144)

[8 Policy Requirements 4](#_Toc68595145)

[8.1 System and Communications Protection Policies and Procedures 4](#_Toc68595146)

[8.2 Application Partitioning 4](#_Toc68595147)

[8.3 Information in Shared Resources 4](#_Toc68595148)

[8.4 Denial of Service Protection 4](#_Toc68595149)

[8.5 Resource Availability 4](#_Toc68595150)

[8.6 Boundary Protection 4](#_Toc68595151)

[8.7 Transmission Confidentiality and Integrity 5](#_Toc68595152)

[8.8 Network Disconnect 5](#_Toc68595153)

[8.9 Cryptographic Key Establishment & Management 5](#_Toc68595154)

[8.10 Use of Cryptography 6](#_Toc68595155)

[8.11 Collaborative Computing Devices 6](#_Toc68595156)

[8.12 Public Key Infrastructure Certificates 6](#_Toc68595157)

[8.13 Mobile Code 6](#_Toc68595158)

[8.14 Voice over Internet Protocol 6](#_Toc68595159)

[8.15 Secure Name/Address Resolution Service (Authoritative Source) 6](#_Toc68595160)

[8.16 Secure Name/Address Resolution Service (Recursive or Caching Resolver) 6](#_Toc68595161)

[8.17 Architecture and Provisioning for Name/Address Resolution Service 7](#_Toc68595162)

[8.18 Session Authenticity 7](#_Toc68595163)

[8.19 Protection of Information at Rest 7](#_Toc68595164)

[8.20 Process Isolation 7](#_Toc68595165)

[8.21 Electronic Mail & PII 7](#_Toc68595166)

# Introduction

Organization Name has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by Organization Name management and in compliance with the Access Control family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of Organization Name systems, facilities, and data are protected. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these policies pertain to all Organization Name employees, contractors, third parties, and others who have access to company and customer confidential information within Organization Name systems and facilities.

# Roles and Responsibilities

These policies apply to all Organization Name employees, contractors, business partners, third parties, and others who need or have access to Organization Name systems and our customer's confidential information.

| **Individual or Group** | **Role** | **Responsibility** |
| --- | --- | --- |
|  | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. |
|  | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program. |
|  | Information Owner | Has statutory, management, or operational authority for Organization Name information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal. |
|  | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Information Security Manager | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Technology Manager | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
|  | Information System Security Officer | Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures. |
|  | System Administrator | Responsible for conducting information system security Administration activities. |
|  | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures |
|  | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

Organization Name and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the Organization Name system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the Organization Name Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
8. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011

# Compliance

Compliance with these policies is mandatory. It is Organization Name policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed annually by an external vendor to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team’s recommendations.

# Policy Requirements

The following system and communications protection requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the information systems.

## System and Communications Protection Policies and Procedures

This document is intended to serve as the *System and Communications Protection Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *System and Communications Protection Policy* and related physical and environmental protection controls have been developed, documented, and disseminated to all applicable personnel.

The Information Owner will review and update the *System and Communication Protection Policy* every three (3) years and the procedure(s) at least annually or any time there are significant changes in software or security. Updates must be made to keep the policy and procedure(s) in alignment with overall business goals and risk position. Any updates, improvements, or suggestions regarding the *System and Communication Protection Policy* and/or procedure(s) must be sent to the Information Owner.

## Application Partitioning

Organization Name must ensure the information system separates user functionality (including user interface services) from information system management functionality.

## Information in Shared Resources

must ensure the information system prevents unauthorized and unintended information transfer via shared system resources.

## Denial of Service Protection

must ensure the information system protects against or limit the effects of distributed denial of service attacks by employing VPC IP restrictions and virtual firewalls. In addition, the information system must create, maintain, and update a list of denial of service attacks that are implemented based on current threats.

## Resource Availability

The information system must protect the availability of resources by allocating defined resources by priority or quota with defined security safeguards.

## Boundary Protection

To protect the information system boundaries, must:

* Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system
* Implement subnetworks for publicly accessible information system components that are logically separated from internal organizational networks
* Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the security architecture
* Limit the number of external network connections to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic
* Implement a managed interface for each external telecommunication service
* Establish a traffic flow policy for each managed interface
* Employ security controls as needed to protect the confidentiality and integrity of the information being transmitted
* Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need
* Review exceptions to the traffic flow policy at least annually
* Remove traffic flow policy exceptions that are no longer supported by an explicit mission or business need
* At managed interfaces, deny network traffic by default and allow network traffic by exception (e.g. deny all or permit by exception)
* Prevent remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks (i.e., ensure VPNs that connect to the information production environment do not allow split-tunneling)
* Route internal communications traffic to external networks through authenticated proxy servers within the managed interfaces of boundary protection devices
* Implement a Host-based Intrusion Detection System (HIDS), or at minimum a host-based firewall on all information servers within the production environment
* Isolate key information security tools, mechanisms, and support components associated with the information system and security administration from other internal information system components via logically separate subnets
* Ensure that information fails securely in the event of an operational failure of a boundary protection device

## Transmission Confidentiality and Integrity

must ensure that the information system protects the confidentiality and integrity of transmitted information by employing cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes of information during transmission unless otherwise protected by alternative physical measures.

## Network Disconnect

must ensure that the information system terminates the network connection associated with a communications session at the end of the session or after thirty (30) minutes for all RAS-based sessions and no longer than sixty (60) minutes for non-interactive user sessions of inactivity.

## Cryptographic Key Establishment & Management

must establish and manage cryptographic keys for required cryptography employed within information in accordance with procedures for generating keys from CA and storing them in a restricted password vault.

Symmetric cryptographic keys must be produced, controlled, and distributed using NIST-approvedkey management technology and processes and approved PKI Class 3 or Extended Validation (EV) certificates and hardware security tokens (if applicable) that protect the user’s private key.

## Use of Cryptography

The information system uses required cryptographic protections via cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance as well as FIPS 140-2-validated cryptography wherever encryption is used to protect unclassified information.

## Collaborative Computing Devices

Collaborative computing devices are not used in the information system environment and are prohibited by .

## Public Key Infrastructure Certificates

must issue public key certificates for session management from an approved service provider.

## Mobile Code

must define acceptable and unacceptable mobile code (e.g. JavaScript, ActiveX, VBScript, etc.) and mobile code technologies and establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies. The use of mobile code within the information system must be authorized, monitored, and controlled.

## Voice over Internet Protocol

If Voice over Internet Protocol (VoIP) technologies are utilized within the information production environment, must establish usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously and authorize, monitor, and control the use of VoIP within the information system.

## Secure Name/Address Resolution Service (Authoritative Source)

must ensure that the information system utilizes DNSSEC for external DNS in order to provide additional data origin authentication and integrity verification artifacts along with the DNS authoritative name resolution data the system in response to external name/address resolution queries.

When operating as part of a distributed, hierarchical namespace, must provide the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

## Secure Name/Address Resolution Service (Recursive or Caching Resolver)

must ensure that the information system utilizes DNSSEC for external DNS in order to perform data origin authentication and data integrity verification on the DNS name/address resolution responses the system receives from authoritative sources when requested by client systems.

## Architecture and Provisioning for Name/Address Resolution Service

must ensure that the DNS systems that collectively provide name/address resolution service for the information system are fault-tolerant and implement internal/external role separation.

## Session Authenticity

must ensure that the information system provides mechanisms to protect the authenticity of communications sessions.

## Protection of Information at Rest

must ensure that the information system protects the confidentiality and integrity of information at rest using cryptographic mechanisms to prevent unauthorized disclosure and modification of customer information on applicable information storage components.

## Process Isolation

must ensure than the information system maintains a separate execution domain for each executing process.

## Electronic Mail & PII

must ensure PII sent over email is sent via a secure function to ensure sensitive information may not be viewed by an unintended recipient.