Insert Logo Here

Organization Name

Security Procedures

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 Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68610756)

[2 Purpose 1](#_Toc68610757)

[3 Scope 1](#_Toc68610758)

[4 Roles and Responsibilities 1](#_Toc68610759)

[5 Management Commitment 2](#_Toc68610760)

[6 Authority 3](#_Toc68610761)

[7 Compliance 3](#_Toc68610762)

[8 Procedural Requirements 4](#_Toc68610763)

[8.1 Application Partitioning, Information in Shared Resources, and Resource Availability 4](#_Toc68610764)

[8.2 Denial of Service Protection 4](#_Toc68610765)

[8.3 Encryption and Key Management 5](#_Toc68610766)

[8.4 Network Disconnect, Trusted Path, Public Access Restrictions, and Session Authenticity 5](#_Toc68610767)

[8.5 Protection of Information at Rest 6](#_Toc68610768)

[8.6 Collaborative Computing Devices 6](#_Toc68610769)

[8.7 Mobile Code 6](#_Toc68610770)

[8.8 Voice Over Internet Protocol 6](#_Toc68610771)

[8.9 Secure Name Address Resolution Services 6](#_Toc68610772)

[8.10 Architecture and Provisioning For Name-Address Resolution Service 6](#_Toc68610773)

[8.11 Process Isolation 7](#_Toc68610774)

# Introduction

 has developed procedures that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These procedures are set forth by 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

This document defines the information system and communications procedures. These procedures are in place to facilitate the implementation of the System and Communications Policy and associated access controls. In accordance with the policy, these procedures detail how information shall implement and maintain secure access controls on all applicable information systems.

# Scope

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

# Roles and Responsibilities

These policies apply to all employees, contractors, business partners, third parties, and others who need or have access to 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 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

 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 system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the 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 procedures is mandatory. It is 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.

# Procedural 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 system.

## Application Partitioning, Information in Shared Resources, and Resource Availability

Organization Name management servers are located within a management subnet and are separated from production systems (which are in additional subnets). The information system uses role-based access control (RBAC), which is managed within {Tool} to provide users their necessary privileges.

Organization Name back-end administrators access the environment via {Tool}, which are on a separate management subnet. The jump servers are only accessible through {Tool}. The jump servers are then used to connect to servers within the environment using the following methods:

* {Connection Methods}
* {Connection Methods}

Front end web application users are logically separated by {Explain}

Information systems are configured to prevent unauthorized and unintended information transfer through shared system resources through logical separation of customer virtual instances. External users and application users do not have direct access to the operating system.

To protect the resource availability, each process has a virtual address space, executable code, open handles to system objects, a security context, a unique process identifier, environment variables, a priority class, minimum and maximum working set sizes, and at least one thread of execution. This is done at the operating system level and is maintained by {IaaS/PaaS Provider}

## Denial of Service Protection

Denial of service (DOS) protection is provided natively by {IaaS/PaaS Provider} in the form of DDOS Protection. This protection provides active traffic monitoring and always-on protection as well as automatic attack mitigations. Organization Name also leverages the {Tools/Description}

Organization Name employs automated mechanisms to monitor and control communications at the external boundary of the system and at key internal boundaries within the information system. The Organization Name web application is only accessible through the {Ingress/Egress Point}. Servers in this environment are only accessible through a secured {RAS/RDP} session through {Tool} via the {Tool}. The {Tool} is limited to only Organization Name administrators who are authorized to have {Tool} privileges.

{Team/Role} can connect directly to {Edge/Jump/Bastion} and no other systems through the {Tool} secured {RAS,RDP} connection. Inside of the information system boundary, {Tools} will be used to limit the allowed traffic between the subnets, including management subnets and data subnets. Traffic is restricted so that connections to external networks are allowed only through managed and secure interfaces.

Only permitted communication ports and protocols are allowed and all communications are denied by default. All traffic flowing to the information system is filtered through firewalls, logged by {SIEM Tool}, and monitored by the Organization Name {Team/Role}. The Organization Name {Team/Role} reviews communication events on a weekly basis.

For interfaces, the information systems employ a “deny-all” approach for network traffic. Any traffic needed support the operation or support of the information system is permitted as an exception to the “deny-all” network traffic rule. The ports protocols and services documentation is reviewed by the {Team/Role}monthly.

Servers, tool systems, databases, and file servers are kept isolated using {Tools} and separate subnets. {Tools} are used to limit traffic from outside the boundary to systems within the boundary.

All components within the information system are configured to fail securely in the event a component failure via {Tools}. {Tools} have implemented validated cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

## Encryption and Key Management

Organization Name protects the confidentiality and integrity of transmitted information by employing cryptographic mechanisms to create secure tunnels between designated endpoints to prevent unauthorized disclosure, monitoring for, and detection of changes during transmission unless otherwise protected by alternative physical safeguards such as protected distribution systems, and placement of information output devices within physical access controlled areas.

Cryptography for {Tools} is managed by {Team/Role}. All cryptographic symmetric keys are 2 validated products. All cryptographic asymmetric keys used are validated products.

{Tools} implement validated cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The organization shall obtain public key certificates under an appropriate certificate policy from an approved service provider.

Cryptographic keys are used to protect the confidentiality and integrity of transmitted information and in the event the key is suspected to be compromised, it must be revoked and replaced. The information system does not permit the use of test keys within the production environment and production keys are not used in a test environment. Any revoked or archived keys are strictly prohibited for new or replacement keys. The {Team/Role} is primarily responsible for enforcing compliance among cryptographic key management.

## Network Disconnect, Trusted Path, Public Access Restrictions, and Session Authenticity

A compliant, multi-factor cryptographic trusted communication path is established between the user and the following security functions of the system:

* System authentication
* Re-authentication

The Organization Name web application ensures that network connections to the information system are terminated at the end of a communication session or after fifteen (15) minutes of inactivity.

## Protection of Information at Rest

Information at rest refers to the state of information when it is located on a secondary storage device (e.g. disk drive or tape drive) within an organizational information system. The {Team/Role} is responsible for defining the physical measures and cryptographic mechanisms to prevent unauthorized disclosure and modification at rest. Currently Protection At Rest (PAR) is accomplished via {AES-128/AES-256} disk encryption in compliance with CIS level 1.

## Collaborative Computing Devices

Organization Name does not implement collaborative computing on system devices.

## Mobile Code

The {Team/Role}, in coordination with the {Team/Role}, defines acceptable and unacceptable mobile code and mobile code technologies that are used within the information system. Currentlythe information system uses the following mobile code within the environment:

* {Mobile Code Type}

Organization Name requires that all mobile code and mobile code technologies be used in accordance with industry best practices, security considerations, and business requirements. Mobile code must be authorized in accordance with the dotStaff SDLC procedure prior to it being used within the environment. Any mobile code not explicitly documented to be authorized is prohibited.

The {Team/Role} approves all mobile code used within the environment. If a developer requires a new mobile code technology, they must obtain approval from the {Team/Role} prior to using it within the environment. The {Team/Role} works together to review new mobile code requests and current mobile code implemented.

## Voice Over Internet Protocol

Usage restrictions and implementation guidance shall be established for any Voice over Internet Protocol (VoIP) technologies used within the information system. The use of VoIP technologies used within the information system shall be authorized, monitored, and controlled. Currently, {no/# of} VOIP Technologies are used within the information system.

## Secure Name Address Resolution Services

Organization Name has implemented DNSSEC by leveraging services provided by {Provider Name} The certificate provided by {Provider Name} for Information Name Resolution is a {Certificate Type}

## Architecture and Provisioning For Name-Address Resolution Service

The information system provides fault-tolerant name/address resolution service. These services are separated by internal and external views that separate roles. Data origin authentication and name/address integrity verification resolution response is received from authoritative sources when requested by information systems components. These services are provided by the implementation of DNSSEC for outbound proxy internet traffic only.

## Process Isolation

Organization Name configures the information system to maintain separate execution domains for each executing process. This is a standard built in processing function of {Operating System Type}