

{Insert CompanY Name}

Security Procedures

SYSTEM AND COMMUNICATIONS

PROTECTION [SC]

**Version:**

{N.N}

**Date:**

{Insert Modified Date}

# Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Any item that needs to be updated within this document can be found with { } around each item and in (RED) Font. [Delete this for final product submission]

# Table of Contents

[Document Revision History 1](#_Toc153285651)

[Table of Contents 2](#_Toc153285652)

[1 Introduction 3](#_Toc153285653)

[2 Purpose 3](#_Toc153285654)

[3 Scope 3](#_Toc153285655)

[4 Roles and Responsibilities 3](#_Toc153285656)

[5 Management Commitment 4](#_Toc153285657)

[6 Authority 5](#_Toc153285658)

[7 Compliance 5](#_Toc153285659)

[8 Procedural Requirements [AC-1] 6](#_Toc153285660)

[8.1 Application Partitioning, Information in Shared Resources, and Resource Availability [SC-2, SC-4] 6](#_Toc153285661)

[8.2 Denial of Service Protection [SC-5] 7](#_Toc153285662)

[8.3 Boundary Protection [SC-7] 7](#_Toc153285663)

[8.4 External Communications Services [SC-7 (4)] 9](#_Toc153285664)

[8.5 Transmission Confidentiality and Integrity [SC-8] 9](#_Toc153285665)

[8.6 Protection of Information at Rest [SC-28] 9](#_Toc153285666)

[8.7 Use of Crytography, Cryptographic Key Establishment & Management, and PKI Certificates [SC-13, SC-12, SC-17] 9](#_Toc153285667)

[8.8 Network Disconnect and Session Authenticity [SC-10, SC-23] 10](#_Toc153285668)

[8.9 Collaborative Computing Devices [SC-15] 10](#_Toc153285669)

[8.10 Mobile Code [SC-18] 10](#_Toc153285670)

[8.11 Voice Over Internet Protocol [SC-19] 11](#_Toc153285671)

[8.12 Secure Name Address Resolution Services [SC-20, SC-21] 11](#_Toc153285672)

[8.13 Architecture and Provisioning For Name-Address Resolution Service [SC-22] 11](#_Toc153285673)

[8.14 Session Authenticity [SC-23] 12](#_Toc153285674)

[8.15 Process Isolation [SC-39] 12](#_Toc153285675)

[8.16 System Time Synchronization [SC-45, SC-45 (1)] 12](#_Toc153285676)

# Introduction

{Insert Company Name} has developed corporate policies that identify the security requirements for its information systems and personnel in order to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by {Insert Company Name}’s 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 5.

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of {Insert Company Name}’s 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 {Insert Company Name} employees, contractors, third parties, and others who have access to company and customer confidential information within {Insert Company Name} systems and facilities.

# Roles and Responsibilities

These policies apply to all {Insert Company Name} employees, contractors, business partners, third parties, and others who need or have access to {Insert Company Name}’s systems and our customer's confidential information. {Insert Company Personnel below and delete this for final product}

|  |  |  |
| --- | --- | --- |
| **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 {Insert Company 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. |
| **Individual or Group** | **Role** | **Responsibility** |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | {Insert Individual or Team Name} | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | 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 Director | 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 Admin Team | System Administrator | Responsible for conducting information system security Administration activities. |
| Varies | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures. |
| Varies | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

{Insert Company 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 {Insert Company Name} Information System by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the {Insert Company 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
2. Federal Information Security Modernization Act of 2014 (FISMA)
3. The Privacy Act of 1974
4. Clinger-Cohen Act of 1996
5. OMB Circulars and Memoranda
6. Federal Information Processing Standards (FIPS)
7. NIST Special Publications
8. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
9. 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 {Insert Company Name}’s 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 by an external vendor and/or internal self-assessments 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 [SC-1]

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 {Insert Company Name} information systems.

**8.1 Application Partitioning, Information in Shared Resources, and Resource Availability [SC-2, SC-4]**

The {Insert Company Name} {Insert Information System Name} Information System is a multi-tiered environment where the {System components such as: *{Insert name of Hosting Provider} Application Gateways, the front-end and API servers, services and utility servers, database servers, Active Directory servers, and management servers*} are contained in separate subnets. Only the ports needed for operation of the {Insert Information System Name} Application and management functions are open between the various subnets. The {Insert Information System Name} Application uses role-based access control (RBAC), which is managed within the {Insert Information System Name} {RBAC database} to provide users their necessary privileges. [SC-2]

{Insert Company Name}’s back-end administrators access the environment via jump servers, which are on a separate management subnet. The jump servers are only accessible through a {Insert how jump servers are accessible, such as: secure Remote Desktop Protocol (RDP)} connection via {Insert RDP Product, such as RDP {Insert name of Hosting Provider} {Insert name of Remote Desktop Tool, such as Bastion}}, which is accessed through the {Insert access methodology, such as {Insert name of Hosting Provider} Portal}. The jump servers are then used to connect to servers within the environment using the following methods:

* {Edit list to fit your organization’s setup}
* Remote Desktop Protocol (RDP)
* PowerShell
* MMC snap-ins (such as the Microsoft Configuration Manager admin console or Event Viewer)
* Web Console for management tools

Front end web application users are logically separated within the database to only access the data in the tenant to which they are assigned.

{Insert Company Name} prevents unauthorized and unintended information transfer by implementing {isolated database instances, unique API keys, and unique sub-domains} for the {Insert Information System Name} Application. Customers do not have direct access to back-end resources and only interact with their unique resources through the {Insert Information System Name} Application. [SC-4]

{Explain how your hosting provider protects your application environment from other customers: 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 {Insert CSP/Virtual Hosting/Hosting Provider} personnel.}

**8.2 Denial of Service Protection [SC-5]**

The {Insert Information System Name} Information System is protected against ICMP (ping) flood, SYN flood, sloworis, buffer overflow attack, volume attack, and various other forms of DDoS attacks. [SC-5 (a)] The information system is protected {Insert Name of Web Application Firewall} along with protection provided natively by {Insert Name of Secondary Protection Provider}. [SC-5 (b)]

**8.3 Boundary Protection [SC-7]**

{Insert Company Name} implements boundary protection using the {Insert list of products/services used to protect the boundary such as: {Insert name of Web Application Firewall} WAF, {Insert name of Hosting Provider} {Insert Name of firewall technology}, {Insert name of Hosting Provider} Application Gateways, and {Insert name of Hosting Provider} {Insert name of Remote Desktop Tool, such as Bastion}}. [SC-7 (a)] No inbound traffic is allowed other than from {Insert name of Web Application Firewall} to the {Insert the name of Front-end tier, gateways, or reverse proxy servers} fronting the {Insert Information System Name} Application. [SC-7 (b)] {Insert Firewall Product Name} control communication between the various {Insert Information System Name} Information System subnets and only permit operationally required ports to communicate between subnets. [SC-7 (c)] {Insert Company Name} limits the number of external network connections to the {Insert Information System Name} Information System by permitting only traffic filtered by {Insert name of Web Application Firewall} to access the {Insert Information System Name} Application. [SC-7 (3)] Additional services are limited to {Insert allowed traffic, such as API} traffic over HTTPS, {Insert name of Scanning/SCAP tool} over encrypted connection, {Insert name of Antivirus Product} antivirus update server and products catalog, {Insert name of Identity provider, such as Okta, if applicable}, {Insert name of external mail service, if applicable} for outbound email, and NIST time service over NTP.

{Insert Company Name} does not use VPN or split tunneling to access components within the boundary. [SC-7 (7)] Servers in the {Insert Information System Name} Information System are only accessible through a secured RDP session through {Insert name of {Insert name of Remote Desktop Tool, such as Bastion} service, such as {Insert name of Hosting Provider} {Insert name of Remote Desktop Tool, such as Bastion}} via the {Insert name of Hosting Provider} Portal. The {Insert name of Hosting Provider} Portal is limited to only {Insert Company Name} administrators who are authorized to have {Insert name of Hosting Provider} Portal privileges. The {Insert name of Hosting Provider} {Insert name of Remote Desktop Tool, such as Bastion} service is configured to only permit administrators to access the jump servers when their traffic originates from the {Insert Company Name} corporate IP address range. System Administrators are allowed to connect directly to jump servers and no other systems through the {Insert name of Hosting Provider} {Insert name of Remote Desktop Tool, such as Bastion} secured RDP connection. Inside of the information system boundary, load balancers, virtual network security groups, and {Insert name of host-based firewall} Firewall (client-side firewall) 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 {Insert name of SIEM tool}, and monitored through {Insert name of SIEM tool} by the {Insert Company Name} {Insert Individual or Team Name}. The {Insert Company Name} {Insert Individual or Team Name} reviews communication events on a weekly basis.

For interfaces, the information systems employ a “deny-all” approach for network traffic. [SC-7 (5)] Any traffic needed to support the operation or support of the SaaS is permitted as an exception to the “deny-all” network traffic rule. The ports protocols and services documentation is reviewed by the {Insert Individual or Team Name} monthly.

{Insert Company Name} utilizes {Insert name of Anti-Malware software or technology} on all {Insert Information System Name} virtual machines within the {Insert Information System Name} Information System which provides HIDS, host-based firewall, web control, and anti-virus. [SC-7 (12)] All {Insert name of Anti-Malware software or technology} alerts are forwarded to {Insert name of SIEM tool} for correlation and analysis by {Insert Company Name} security personnel.

{Insert Company Name} has created a dedicated management subnet used by {Insert list of management tools found in the dedicated management virtual network} and {Insert name of Scanning/SCAP tool}; a separate dedicated management subnet for {Insert Name of directory services technology, such as Active Directory domain controllers}; and a management network that is further partitioned into the {Insert name of Hosting Provider} {Insert name of Remote Desktop Tool, such as Bastion} subnet, the jump server subnet, and container subnet. [SC-7 (b)] Communication between management services and the various applications subnets are controlled by {Insert name of Hosting Provider} {Insert Name of firewall technology}. The {Insert Information System Name} Information System is configured to fail safely by using {Insert name of protection technology} configuration settings. [SC-7 (18)] In the event there is an operational failure of a boundary protection device the {{Insert name of protection technology} Gateway and {Insert name of protection technology} Load Balancer closes all ports into the {Insert Information System Name} Application. The ports will remain closed until the {Insert Individual or Team Name} reenables the ports, following restoration of the boundary protection device.

Any inbound and the resulting outbound web application traffic to and from the {Insert Information System Name} Application servers is routed through {Insert name of Web Application Firewall}. {Insert name of Web Application Firewall} decrypts and inspects inbound and outbound traffic destined to and from the {Insert Information System Name} web application servers utilizing the following inspection rule types: [SC-7 (8)]

{Update list to include types of protection enabled.}

* {DDoS Attacks}
* {Cross-site Scripting (XSS)}
* {SQL Injection}
* {Directory Traversal}
* {Protocol enforcement}
* {Remote code execution}
* {Known exploit prevention / “Script Kiddies”}
* {Blocks on embargoed countries}

**8.4 External Communications Services [SC-7 (4)]**

{Insert Company Name} relies on {Insert name of hosting provider} to maintain external telecommunications services including {Insert list of external telecommunications services maintained. Example: Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols}.

**8.5 Transmission Confidentiality and Integrity [SC-8]**

The {Insert Information System Name} Information System, including front-end web access and {Insert name of Hosting Provider} {Insert name of Remote Desktop Tool, such as Bastion} access, uses HTTPS (TLS 1.2 or higher) to protect the confidentiality and integrity of data in transit. [SC-8] The {Insert Information System Name} Information System servers are configured in accordance with DISA STIGs and FIPS 140-2 {approved | validated} cryptographic algorithms. [SC-8 (1)]

**8.6 Protection of Information at Rest [SC-28]**

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 {Insert Individual or Team Name} is responsible for defining the physical measures and cryptographic mechanisms to prevent unauthorized disclosure and modification at rest. [SC-28] The {Insert Information System Name} Information System’s file, database, and web servers are configured in accordance with DISA STIGs. [SC-28 (1)] All servers require hard drive encryption or managed disk using AES 256 encryption. {Insert Information System Name} Application databases are backed up to {Insert name of Hosting Provider} Storage accounts using AES 256 encryption. The {Insert Information System Name} Infrastructure is backed up to {Insert name of Offsite Backup Service}.

**8.7 Use of Crytography, Cryptographic Key Establishment & Management, and PKI Certificates [SC-13, SC-12, SC-17]**

{Insert Company 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. For data in transit, including front-end web access and {Insert name of Remote Desktop Tool, such as Bastion} access, the {Insert Information System Name} Information System uses HTTPS (TLS 1.2 or better) to protect the confidentiality and integrity of transmitted information. {Insert Information System Name} servers are configured in accordance with DISA STIGs and FIPS 140 or NSA approved cryptographic algorithms. A detailed list of cryptographic module utilization within the {Insert Information System Name} boundary can be found in the control implementation statement for SC-13 in the System Security Plan document. [SC-13]

{Insert Company Name} uses {Insert name of Key Storage Product} to establish and manage cryptographic keys for required cryptography employed within {Insert Information System Name}. [SC-12] {Insert Company Name} leverages {Insert name of certificate authority} for RDP and server communication. [SC-17 (b)] New keys are generated and destroyed via {Insert name of key generating facility}. Keys are accessed via {Insert access methodology such as: API calls} to the {Insert name of Key Storage Product} where they are stored and encrypted with {Insert protection mechanism such as AES-256 cryptographic algorithms}. {Insert Company Name} uses {Insert name of Key Storage Product} to produce, control, and distribute asymmetric cryptographic keys. [SC-17 (a)]

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 {Insert Individual or Team Name} is primarily responsible for enforcing compliance among cryptographic key management.

**8.8 Network Disconnect and Session Authenticity [SC-10, SC-23]**

The {Insert Information System Name} Information System terminates network connection associated with a communications session at the end of the session or after ten (10) minutes of inactivity for privileged sessions and no longer than fifteen (15) minutes of inactivity for remote-based sessions via {Insert how this is enforced such as Active Directory Group Policy}. User inactivity timeout for the {Insert Information System Name} application is set to fifteen (15) minutes. [SC-10]

{Insert Company Name} uses the TLS 1.2 (or greater) cryptographic protocol, which is resistant to man in the middle attacks. {Insert Company Name} uses digital certificates to establish the identity of jump boxes as the access point to the {Insert name of Hosting Provider} environment. Digital certificates are used in public key cryptography (PKI) to establish the identity of a server or client for the purposes of authentication. [SC-23]

**8.9 Collaborative Computing Devices [SC-15]**

Collaborative computing devices, protocols, or transmissions are not authorized for use or enabled for any system components within the {Insert Information System Name} Information System.

**8.10 Mobile Code [SC-18]**

The {Insert Individual or Team Name}, in coordination with the {Insert Information System Name} Development Team, defines acceptable and unacceptable mobile code and mobile code technologies that are used within the {Insert Information System Name} Information System. Any mobile code not explicitly documented to be authorized is prohibited. [SC-18 (a)] Currently, the {Insert Information System Name} Application uses the following mobile code within the environment:

{Update list to include types of authorized mobile code.}

* {JavaScript Binaries}
* {Xamarin Mobile code}

{Insert Company 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 {Insert Information System Name} SDLC procedure prior to it being used within the environment. Any mobile code not explicitly documented to be authorized is prohibited.

The {Insert Individual or Team Name} approves all mobile code used within the environment. If a developer requires a new mobile code technology, they must obtain approval from the {Insert Information System Name} {Insert Individual or Team Name} prior to using it within the environment. The {Insert Company Name} {Insert Individual or Team Name} monitors the current mobile code technologies in use and recommends updates as needed. [SC-18 (b)]

**8.11 Voice Over Internet Protocol [SC-19]**

VoIP technologies are not used or enabled in any capacity within the {Insert Information System Name} Information System. {Insert Company Name} does not allow the use of VoIP technologies within the {Insert Information System Name} Information System boundary.

**8.12 Secure Name Address Resolution Services [SC-20, SC-21]**

DNSSEC keys for name resolution are Class 3, providing DNSSEC and issued by the {Insert name of certificate authority used for DNSSEC} certificate authority. {Insert name of external DNSSEC provider} provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries. [SC-20 (a)] {Insert name of external DNSSEC provider} provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. [SC-20 (b)]

The {Insert Information System Name} Information System uses {Insert name of external DNSSEC provider} to request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. Internal DNSSEC utilizes {{Insert name of internal DNSSEC provider}}. [SC-21]

Once public DNSSEC is configured, the configuration is validated utilizing <https://viewdns.info> or the Sandia National Labs (<https://dnsviz.net>) tools.

**8.13 Architecture and Provisioning For Name-Address Resolution Service [SC-22]**

The {Insert Information System Name} Information System provides fault-tolerant name/address resolution service. The {Insert name of Internal DNSSEC} DNS service is installed on all {Insert Name of directory services technology, such as Active Directory domain controllers} within the information system providing for fault tolerance and redundancy for internal DNS resolution. {Insert name of external DNSSEC provider} DNS Services provide fault tolerance and redundancy for external DNS resolution via the configuration and deployment to {Insert information on how the external provider achieves fault tolerance and redundancy}. [SC-22]

**8.14 Session Authenticity [SC-23]**

{Insert Company Name} uses the TLS 1.2 (or greater) cryptographic protocol, which is resistant to man in the middle attacks. {Insert Company Name} uses digital certificates to establish the identity of jump boxes as the access point to the {Insert name of Hosting Provider} environment. Digital certificates are used in public key cryptography (PKI) to establish the identity of a server or client for the purposes of authentication. [SC-23]

**8.15 Process Isolation [SC-39]**

{Insert Company Name} configures the information system to maintain separate execution domains for each executing process. {Insert Company Name} utilizes {Insert list of operating systems} (or greater) in the {Insert Information System Name} Information System and maintains default operating system settings for process isolation, which is native to {Insert list of operating systems} Operating Systems. The {Insert Information System Name} Web Application uses individual application pools to isolate web applications on a single server. [SC-39]

**8.16 System Time Synchronization [SC-45, SC-45 (1)]**

The {Insert internal Network Time Protocol sources servers} are configured to synchronize their clock times with the NIST authoritative time sources, documented at <http://tf.nist.gov/tf-cgi/servers.cgi>, at least hourly; all other servers in the environment sync their time from the domain controllers. [SC-45] [SC-45 (1) (a)] All servers use NTP to maintain time synchronization, and if the time difference is greater than zero (0), it forces a resync immediately. [SC-45 (1) (b)]