

{Insert Company Name}

Security Procedures

ACess Control (AC)

**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 {Insert...} around each item and in (RED) Font. [Delete this for final product submission]

# Table of Contents

[Document Revision History 1](#_Toc152931652)

[Table of Contents 2](#_Toc152931653)

[1 Introduction 4](#_Toc152931654)

[2 Purpose 4](#_Toc152931655)

[3 Scope 4](#_Toc152931656)

[4 Roles and Responsibilities 4](#_Toc152931657)

[5 Management Commitment 5](#_Toc152931658)

[6 Authority 6](#_Toc152931659)

[7 Compliance 6](#_Toc152931660)

[8 Procedural Requirements [AC-1] 7](#_Toc152931661)

[8.1 Account Management [AC-2] 7](#_Toc152931662)

[8.1.1 Account Identification 7](#_Toc152931663)

[8.1.2 Adding New Users 7](#_Toc152931664)

[8.1.3 Removing Terminated or Transferred Users 9](#_Toc152931665)

[8.1.4 Current Users 10](#_Toc152931666)

[8.1.5 Shared & Group Accounts 10](#_Toc152931667)

[8.1.6 Temporary & Emergency Accounts 10](#_Toc152931668)

[8.2 Audting of Accounts [AC-2 (7), AC-2 (4)] 10](#_Toc152931669)

[8.3 System and Account Parameters [AC-2 (5)] 11](#_Toc152931670)

[8.4 System Use Notification / System Warning Banner [AC-8] 11](#_Toc152931671)

[8.5 Information Flow Enforcement [AC-4, AC-4] 12](#_Toc152931672)

[8.6 Separation of Duties and Least Privilege [AC-5, AC-6] 12](#_Toc152931673)

[8.7 Unsuccessful Login Attempts [AC-7] 13](#_Toc152931674)

[8.8 Session Lock and Termination [AC-11, AC-12] 14](#_Toc152931675)

[8.9 Permitted Actions Without Identification or Authentication [AC-14] 14](#_Toc152931676)

[8.10 Remote Access [AC-17] 14](#_Toc152931677)

[8.10.1 Remote Access Authorization and Connection Requirements 14](#_Toc152931678)

[8.10.2 Remote Access Monitoring [AC-17 (1)] 15](#_Toc152931679)

[8.10.3 Remote Access Integrity and Confidentiality [AC-17 (2)] 15](#_Toc152931680)

[8.10.4 Remote Access Connection Disconnect 15](#_Toc152931681)

[8.11 Configuring Wireless Access [AC-18] 15](#_Toc152931682)

[8.12 Configuring Mobile Access [AC-19] 15](#_Toc152931683)

[8.13 External Information Systems and Information Sharing [AC-20, AC-21] 15](#_Toc152931684)

[8.14 Publicly Accessible Information [AC-22] 16](#_Toc152931685)

[9 Addendum A: List of Users Permitted to Access the Datacenter 18](#_Toc152931686)

[10 ADDENDUM: List of Users with Remote Access Privileges 19](#_Toc152931687)

[11 Addendum C: List of Users With Publicly Accessible Content Privileges 20](#_Toc152931688)

[12 Addendum D: List of Current External Information Systems 21](#_Toc152931689)

# 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 Information Security leadership role 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 [AC-1]

The following access control Security 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 Account Management [AC-2]

{Insert Company Name} personnel shall establish, activate, modify, disable, and remove accounts in accordance with the procedures herein. [AC-2 (f)]

8.1.1 Account Identification

The Information Security Manager must annually review the following types of {Insert Product Name} Information System accounts to support organizational missions/business functions: [AC-2 (a)]

* {Insert Name} Resource Portal
* {Insert Product Name} Infrastructure
* {Insert Product Name} Application

Service accounts are created and managed through the Change Management Board and system Administrators use Active Directory to support the management of system accounts in accordance with the procedures herein.

All {Insert Product Name} Information System accounts are monitored via {Insert SIEM Name}. {Insert Directory Service} collects account usage logs. The events are reviewed and monitored in {Insert SIEM Tool}. Client and vendor owned accounts are the responsibility of the client and vendor to monitor use respectively. [AC-2 (g)]

8.1.2 Adding New Users

For the back-end {Insert Product Name} accounts and {Insert Directory Service Name or CSP} accounts, account creation requests are documented in the {Insert Company Name} {Insert Directory Service} ticketing system, which is an implementation of {Insert Name}, and are approved by the {Insert IT leadership role name} or delegate(s) and {Insert Role} or delegate(s).

For privileged {Insert Product Name} application accounts, account creation requests are documented in the {Insert Company Name} {Insert Directory Service Name} ticketing system and are approved by the Product Owner, implemented by the {Insert IT leadership role name} or delegate(s), and monitored by the {Insert Information Security leadership role name} or delegate(s). [AC-2 (e)]. Once approval is granted, the new user can be added to the system.

Prior to being added to an existing group or role, users obtaining administrative or privileged accounts are required to satisfy the following prerequisites: [AC-2 (c)]

* Complete group or role specific training
* The staff member’s job functions require access to back-end {Insert Product Name}, {Insert Name} Portal, and/or {Insert Product Name} application accounts

New user accounts are assigned in the following systems:

* {Insert Company Process for General User}
* {Insert Company Process for Admin}

{Insert Company Name} authorizes access to the {Insert Product Name} information system based on:

* {Insert Directory Service Tool Name}
* {Insert Specific Area}

The table below outlines the different account types and various access privileges defined by role. [AC-2 (d)] [AC-2 (i)]

|  |  |  |
| --- | --- | --- |
| **Account Type** | **Role** | **Access Description** |
| {Insert Name} **Back-end Account** | System Administrator | Has domain level privileges for full administrative access to servers in the {Name of System} security boundary. |
| Database Administrator | Has full administrative access to the databases inside the {Name of System} security boundary. |
| Information Security Administrator | Has local administrative permissions on the servers to administer {Insert Name} |
| {Insert Name} Configuration Manager Administrator | Has local administrative permissions on the servers to apply patches and deploy software installations. |
| Resource Administrator | Has the ability to create and edit {Insert Name}-based resources such as provisioning a server or accessing network security groups or application services. |
| Global Administrator | Has full ownership rights to all tenants, the hosting tenant, and resources inside the account as well as billing and capacity permissions. |
| {Insert Name}  **Web Account** | {Insert Name} Admin | Has full access to update financial information, account data, and any other data fields within the application. The {Insert Name} Admin also has the ability to create, modify, and delete other accounts. For a complete description of the account permissions, see the *Separation of Duties Matrix*. |
| {Insert Role} | In a client support capacity, the account holder is authorized to make changes to users and data within the client’s tenant. For a complete description of the account permissions, see the *Separation of Duties Matrix*. |
| **Government Customer Account** | Client Admin | Can access and change data within their instance of the application. For a complete description of the account permissions, see the *Separation of Duties Matrix*. |
| Client User | Limited to their own project and resource information, or information for which they have been given access by the Client Administrator. For a complete description of the account permissions, see the *Separation of Duties Matrix*. |
| Vendor User | Can access and change data within their instance of the application. For a complete description of the account permissions, see the *Separation of Duties Matrix*. |
| Vendor Admin | Limited to their own project and resource information, or information for which they have been given access by the Vendor Administrator. For a complete description of the account permissions, see the *Separation of Duties Matrix*. |
| Resource or Contractor | Limited to editing their own account information. For a complete description of the account permissions, see the *Separation of Duties Matrix*. |

Account Managers are created for all account types. Only the individuals listed below are authorized to act as an Account Manager for the specified account type. [AC-2 (b)]

* For {Insert Role Name} Infrastructure Accounts, only the IT Manager and/or Information Security Manager may act as an Account Manager.
* For {Insert Role Name} Applications Accounts, only the Development Product Owner and/or Information Security Manager may act as an Account Manager.
* For {Insert Role Name} Resource Portal Accounts, only the IT Manager and/or Information Security Manager may act as an Account Manager.
* For Federal Government Customer Accounts, only the client Authorizing Official, the client’s security team, or a designated official may act as an Account Manager.

Automatic emails, triggered by an onboarding or offboarding ticket in {Directory Service Tool}, are sent to the appropriate {Insert Company Name} IT and Information Security personnel when an employee has been hired. [AC-2 (1)] Once a new user account has been created, a notification will be sent to the user containing their login credentials.

8.1.3 Removing Terminated or Transferred Users

When a user account is deleted due to termination or transfer, all access privileges must also be removed. If a user is transferring and needs or no longer needs certain privileges, the employee’s previous manager and new manager must submit an {Directory Service Tool} ticket to request the specific privileges be added to or removed from the user account. [AC-2 (l)] [AC-2 (7) (d)]

Upon completion of user account changes, a notification will be sent to the user and reporting manager stating that the user’s privileges have been updated. Account managers are notified of these changes through the {Directory Service Tool} ticketing system within: [AC-2 (h)]

* Twenty-four (24) hours when the account is no longer required [AC-2 (h) (1)]
* Eight (8) hours when the {Company Role} Information System user is terminated or transferred [AC-2 (h) (2)]
* Eight (8) hours when the {Company Role} Information System usage or need-to know/need-to-share changes [AC-2 (h) (3)]

In the event of privilege removal, the System Administrators use {Directory Service Process}, or {Directory Service Tool} to update the user’s privileges, depending on from which system the privilege is being removed. This action is performed when an Administrator receives an approved request, during the annual account review, or during quarterly privileged account reviews.

Automatic emails, triggered by an onboarding or offboarding ticket in {Directory Service Tool}, are sent to the appropriate {Insert Company Name} IT and Information Security personnel when an employee has been terminated. [AC-2 (1)]

8.1.4 Current Users

The Information Security Manager, IT Manager, and Development Product Owner review all privileged accounts on a quarterly basis by retrieving lists of accounts from {Insert Directory Service Process}, {Insert Directory Service Tool Name}, and Internal {Process}, and comparing them with employees’s current roles and privileges. All other accounts are viewed annually. [AC-2 (j)] {Insert Company Name} has implemented domain policies in {Insert Name of Directory Service Tool} and the Internal {Insert Name of Directory Service Tool}, as well as in {Insert Role} user policy assignments to ensure the information system is configured to disable inactive user accounts after ninety (90) days. [AC-2 (3) (d)] {Insert Product Name} Infrastructure and {Insert Product Name} Application user accounts are disabled within twenty-four (24) hours:

* After accounts have expired, [AC-2 (3) (a)]
* When accounts are no longer associated with a user or individual, [AC-2 (3) (b)] and/or
* If the account is in violation of {Insert Company Name} policy [AC-2 (3) (c)]

8.1.5 Shared & Group Accounts

{Insert Company Name} {select one: does or does not} utilize shared and/or group accounts. [AC-2 (9)] [AC-2 (k)]

8.1.6 Temporary & Emergency Accounts

{Insert Company Name} utilizes Emergency Accounts for {Insert Role} and {Insert Role(s)}. The first emergency account, the MFA credentials are not known, and they are stored, along with the hardware token, physically in a safe where only the CEO of the company is aware of the combination. The second account is protected by MFA application that only the IT director and IT Manager have access. If a new temporary or emergency account is added, similar controls will be added to that new account. In the event any of the temporary or emergency accounts are used, the password is changed within 96 hours of the last use, so that the credentials are no longer readily known by any party. [AC-2 (2)]

8.2 Audting of Accounts [AC-2 (7), AC-2 (4)]

Logging is enabled within {Name of Directory Service Process} and {Directory Service Tool Name} to build events for the creation of all new accounts, changes in account access, account disable, or account termination actions for the {Insert Product Name} Infrastructure using {SIEM}. The Information Security Team reviews {SIEM Tool Name} and {SIEM Logging Tool} weekly for these log event types. Alerts are created within {SIEM Tool Name} and sent as emails to the Information Security Team. [AC-2 (4)]

For any account changes, the Information Security Team will verify that either an {Directory Service Tool} Support Request regarding user permissions, or a Change Management request regarding a service account is associated with the event.

If an {Directory Service Tool} Support Request or a Change Management request does not exist, the Information Security Team will disable the account and begin an investigation in coordination with the IT Team regarding the account’s creation. Corrective actions and/or activation of the Incident Response Plan (IRP) are relevant outcomes, as well as remediation training on process, if deemed appropriate.

All privileged role assignments are recorded and monitored in {Directory Service Tool/Process}. [AC-2 (7) (b)] Privileged user accounts are monitored by the Information Security Team for unusual behavior including accessing accounts from locations that are not considered normal using {Directory Service Tool} and {SIEM}. The Information Security Team reports questionable usage of privileged accounts to the Development and IT Teams to investigate. [AC-2 (12)]

If an individual is discovered to be involved in activities that have adverse impacts to organizational operations, organizational assets, individuals, other organizations, or the Nation, the account will be disabled, within the {Insert Product Name} Infrastructure and the {Insert Product Name} Application, within one (1) hour of that discovery. [AC-2 (13)]

8.3 System and Account Parameters [AC-2 (5)]

{Insert Company Name} has implemented the following system and account security requirements and parameters:

* {Insert Company Name} requires that privileged users log out at the conclusion of their workday. [AC-2 (5)]
* {Directory Service Tool}, Internal {Directory Service}, and {SIEM} are configured to enforce lockout limits to be set to three (3) invalid login attempts within a fifteen (15) minute time period.
* Mechanisms are employed to automatically lock a user session after fifteen (15) minutes of inactivity and systems shall retain the session lock until the user reestablishes access using authenticated means of reconnection with valid username and password.
* Upon session lock, assets shall be configured to conceal information system information previously visible on the display with a publicly viewable image.
* In accordance with DISA STIG requirements, accounts will auto-unlock fifteen (15) minutes after an account lockout occurs.
* In accordance with the {Insert Company Name} *Rules of Behavior* and *Acceptable Use Policy*, all users are required {Describe Method Used} to execute a lock function and lock their computer when they expect to be away from their workstation.
  + Violation of this policy is subject to disciplinary actions in accordance with the {Insert Company Name} *Rules of Behavior* and *Acceptable Use Policy*.
* Each account or account type should be limited to certain number of concurrent sessions
  + Under the Windows domain policy, accounts are configured to limit concurrent sessions. Non-privileged accounts are limited to three (3) sessions, privileged accounts are limited to two (2) sessions.
  + Infrastructure/Management sessions: Limited via windows-native constraints via RDP to jump servers to one privileged session. Non-privileged accounts do not exist for back-end management.
  + Application sessions: Limited to two sessions for all account types.

8.4 System Use Notification / System Warning Banner [AC-8]

{Insert Company Name} enforces the user of a system “warning” banner which displays privacy and security notices including the statements listed below. The banner will remain displayed on the screen until users manually select the “Accept” or “OK” button to proceed with the log in process.

* Users are accessing a U.S. Government information system
* The information system usage may be monitored, recorded, and is subject to audit
* Unauthorized use of the information system is prohibited and subject to criminal and civil penalties
* Use of the information system indicates consent to monitoring and recording
* For the publicly accessible web application, system use information and warning banner is displayed beneath the statement “By logging in an above, you agree to the below statement.” Consent with the system use requirements is granted when the user logs in to the system.

8.5 Information Flow Enforcement [AC-4, AC-4]

The IT Team and the Information Security Team determine information flow implementation. Information flow is controlled, and approved authorizations are enforced by: [AC-4]

* Filtering and routing policies on {Network Security Groups SIEM Tool(s) SIEM Tool Name} (e.g., Firewall rules, Load Balancers, VPN gateways, App gateways, VNets, and internal VNet subnets). [AC-4 (21)]
* Using {Directory Service Tool(s)} (e.g., security groups, write, execute, permissions assigned to roles, folders, and/or files and databases) through access control lists.
* Enforcing access control to the information system through {Directory Service Tool(s)} (e.g., security groups, roles, unique User IDs and passwords, multi-factor authentication, and access rights) based on the least privilege principle. [AC-3]
* Separating information flow logically using {SIEM Tool(s)} (Define Company Process) that limit traffic to provide complete separation of customer tenants and data.

8.6 Separation of Duties and Least Privilege [AC-5, AC-6]

Separation of Duties is designed to avoid conflicts of interest or prevent control failures that could result in abuse, fraud, data theft, or security breaches. A properly implemented Separation of Duties prevents malicious activity without collusion. Least privilege is designed so that an individual only has access to the systems and tools they need to perform their job.

{Insert Company Name} utilizes {Directory Service Tool} to enforce separation of duties and least privilege by creating standardized roles that only have the entitlements required to perform a specific job function and assigning individual accounts to those standardized roles. [AC-5 (a)] [AC-6] [AC-2 (7) (a)] {Insert Company Name} ensures that various roles are assigned to different personnel and personnel are not assigned responsibilities intended for other job functions. The {Insert Company Product Name} Information System implements {Directory Service Tool} using {Directory Service}, Internal {Directory Service}, {Insert Name} Universal Directory, and SQL Groups to manage the entitlements of different user roles. Roles such as System Administrator, Information Security, Database Administrator, Network Administrator, {Insert Product Name} Administrator, and {Insert Other Role Names} are carried out by separate individuals. Individuals are monitored through system and security event records and the {Insert SIEM Tool(s) and Directory Service} for changes in roles or attributes regarding their role. [AC-2 (7) (c)]

{Insert Company Name} utilizes an {SIEM Tool(s)} table to record and keep track of the privileges of the roles within the {Insert Product Name} Information System. The {SIEM Tool(s)} table is reviewed annually for validation, [AC-6 (7) (a)] and privileges are reassigned or removed, if necessary. [AC-6 (7) (b)]

Non-privileged user accounts do not have permissions to modify users, reassign tasks, or modify workflow processes. Only limited IT Support staff have {Directory Services Data} Administrative access. For complete permissions details, see the Separation of Duties Matrix.

The following separation of duties policies are to be maintained at all times:

* Duties are explicitly assigned as needed to meet organizational objectives, ensuring the separation of duties is documented. [AC-6 (1)]
* Information system access authorizations are documented in {Insert Company Name} {Directory Service Tool(s)} to support the separation of duties and individual duties will be managed through the Access Control Policy, role membership, and permission settings [AC-5 (b)]
* Roles and groups within the system {SIEM Tool(s)} govern what users are able to see and do through {Directory Service Database} (e.g., security group memberships, specific database permissions, and application roles). Features and functions of the system are only available to select users based on job function.
* Privileged accounts are restricted to IT and Information Security Team staff in order to limit access and securely operate the information system. [AC-6 (5)]
* When IT and Information Security Team staff are performing non-administrative functions, they are required to use a unique, non-privileged account. [AC-6 (2)]
* The assignment of responsibilities required to support the network, applications, and systems are split into multiple {Directory Service Database Role} roles defined in the Separation of Duties Matrix.
* Individuals do not have access permissions to devices, systems, and applications outside of their support responsibilities.
* Non-privileged users are prevented, via the {OS, Directory Service, Roles, Policy’s, and Application settings}, from executing privileged functions including disabling, circumventing, or altering implemented security safeguards or countermeasures. [AC-6 (10)]
* {SIEM Logging Tool(s)} and automated logging mechanisms are used to audit and monitor the execution of privileged accounts. [AC-6 (9)]
  + {SIEM Tool(s)} every instance where a privileged account is used or makes a change
  + {SIEM Tool(s)} has been configured with dashboards to monitor for the following events within {SIEM Tool(s)}:
    - Establishing system accounts
    - Configuring access authorizations (e.g., permissions, privileges)
    - Changes to event policy
    - System and security administration
    - When account permissions are changed
    - When a new administrative account is created
    - Other privileged functions

8.7 Unsuccessful Login Attempts [AC-7]

Users are limited to three (3) consecutive invalid log in attempts during a fifteen (15) minute time period. If the user exceeds the maximum number of unsuccessful log in attempts, the account/node will be automatically locked for thirty (30) minutes and delays the next logon prompt for fifteen (15) minutes.

{Insert Company Name}’s IT Team enforces a limit of no more than three (3) consecutive invalid login attempts by a user within a fifteen (15) minute period. The Information Security team gives the IT Team the parameters, and the IT Team applies the policy to {Directory Service} via {Directory Service Database} policy and {SIEM Tool(s)}.

The IT Team configures {Directory Service Tool(s)} group policy to lock out the accounts and delay the next log in attempt for a half an hour when the maximum number of unsuccessful attempts is exceeded.

8.8 Session Lock and Termination [AC-11, AC-12]

For the {Insert Product Name} Application, the screen frosts over [AC-11 (1)] after fifteen (15) minutes of inactivity and prompts the user if they are still there. If they do not reply within five (5) minutes of that prompt, the session terminates and requires reauthentication. [AC-11] The {Insert Product Name} Application also terminates the session after receiving a logout request from the user. [AC-12]

For servers, the session lock is configured via {Directory Service Tool(s)} to lock a session after fifteen (15) minutes of inactivity [AC-12], blank the screen [AC-11 (1)], and require reauthentication to resume the session. {Insert Company Name} also requires users to lock their device before leaving the device unattended. [AC-11] The servers also terminate the session after receiving a logout request from the user. [AC-12]

For administrative front-end web access, session lock is configured via {Directory Service Tool(s)} to display a screensaver [AC-11 (1)] after fifteen (15) minutes on systems and requires reauthentication to resume the session. [AC-11] The system also terminates the session after receiving a logout request from the user. [AC-12]

8.9 Permitted Actions Without Identification or Authentication [AC-14]

All actions permitted within the web application and back-end access require identification and authentication to access the appropriate system. Other than viewing logon prompts and the warning banner or opening a support request, all actions within the {Insert Product Name} Information System require identification and authentication.

8.10 Remote Access [AC-17]

Remote access to the {Insert Product Name} Infrastructure is established through {SIEM Tool(s)} and {Directory Service Tool(s)}. Direct access to the {Insert Product Name} Infrastructure is not permitted through any means other than {SIEM Tool(s)} through the {Directory Service Tool(s)}. [AC-17 (a)] The following sections give details on the implementation and protection of the remote access solution.

8.10.1 Remote Access Authorization and Connection Requirements

{Insert Product Name} Information Security Team members and IT Team members are the only personnel permitted to remote access into the {Insert Product Name} Infrastructure. For a member of either team to be provisioned, their manager requests access through the {Insert SIEM Tool(s) or Account Request Process}. Requests must be approved by the {Insert IT leadership role name} or delegate(s) and {Insert Information Security leadership role name} or delegate(s) before remote access is granted.

Both IT and Information Security personnel are added to the {Directory Service Database} Security Group. Access to the {Directory Service Database} Resource Portal requires username and password via {Directory Service Tool(s)} and MFA via {Insert MFA Device Name}. Once an administrator has successfully authenticated via Username, Password and {Insert MFA Device} via the {Directory Service Database} Resource portal [AC-17 (b)], the user utilizes the {Directory Service Tool(s)} service to access their appropriate server utilizing their {Insert Product Name} domain credentials for the targeted instance. {Directory Service Server} is configured to only allow access to the {Type of Server} servers, access to all other servers directly through {Directory Service Tool} is blocked. [AC-17 (3)]

8.10.2 Remote Access Monitoring [AC-17 (1)]

The Information Security Team uses {Directory Service Tool(s)} to monitor remote access. {Directory Service Tool(s)} ingests {Directory Service Database} Resource Portal logs and the Information Security team reviews those logs weekly for anomalies such as unauthorized access and privileged escalation. The IT Team uses {Directory Service Tool(s)} security groups in {Directory Service Database} to automate control of remote access to {Directory Service Tool(s)}.

8.10.3 Remote Access Integrity and Confidentiality [AC-17 (2)]

Connections with {Directory Service} Portal, {Directory Service Database}, and {SIEM Tool(s)} Remote Desktop Protocol within the {Insert Product Name} Information System are configured to require TLS 1.2 (or higher) encryption to protect the confidentiality and integrity of remote desktop sessions.

8.10.4 Remote Access Connection Disconnect

Execution of privileged commands and access to security-relevant information via remote access are only authorized for {Define Environment Type} (e.g., Live Test, Production, etc.) environment support through the {SIEM Tool(s)} Portal using {Directory Service Tool(s)}. These connections are logged and monitored via {SIEM Tool(s)}. [AC-17 (4) (a)] The rationale for providing authorization is documented in the {Insert Product Name} Information System, (System Security Plan (SSP)). [AC-17 (4) (a)].

{Insert Company Name} IT and Information Security Team members with {Directory Service Resource Portal} administrative privileges have the capability to immediately disconnect or disable remote access by turning the capability off in the {Directory Service Database}.

8.11 Configuring Wireless Access [AC-18]

{Insert Company Name} only permits configured and hardened wireless networks that use authentication protocols that provide authenticator protection and mutual authentication access points to be used for work purposes.

8.12 Configuring Mobile Access [AC-19]

{Insert Company Name} policy only permits {Define Organization Level} configured and hardened laptops to be used for work purposes. {Insert Company Name} laptops are hardened with full disk encryption. No other portable or mobile devices are permitted.

8.13 External Information Systems and Information Sharing [AC-20, AC-21]

{Insert Company Name} does not allow external systems to access the {Insert Product Name} Information System. [AC-20 (1) (a)] [AC-20 (1) (b)] In the event that external systems need access to {Insert Product Name}, the following will apply: [AC-20 (a)]

* The external system must be StateRAMP Authorized at the moderate level.
* An appropriate interconnection security agreement is provided and approved by the tenant agency.
* A formal and documented access request has been submitted and terms and conditions setting the scope of the access have been agreed upon and approved by the {Insert Information Security leadership role name} (or delegate) prior to access being granted to the external system.
* The Information Security Team shall retain connection or processing agreements with the external entity and validate that the external information systems have the following security controls in place:
  + The latest operating system security patches
  + Current antivirus/antimalware software
  + Support of FIPS140-2 approved encryption for connection to the information system
  + A means of auditing and alerting
* Any findings regarding the external information system’s security controls will be documented and retained. {Insert Company Name} may require findings to be remediated prior to allowing the external information system connection.

[(This section must be adjusted to meet your company’s policy) {Insert Company Name} prohibits accessing the {Insert Product Name} Information System from embargoed countries and countries known for state sponsored cyber threats. {Insert Company Name} blocks the processing, storing, or transmitting organization-controlled sensitive information on prohibited systems outside of the United States using the {Directory Service Tool(s)} Firewall. [AC-20 (b)] The use of {Insert Company Name} controlled portable storage devices by authorized individuals on external information systems is prohibited without explicit authorization from the {Insert Company Name} {Insert Information Security leadership role name} or delegate. [AC-20 (2)]]

The {Insert Company Name} {Insert Information Security leadership role name} or Information System Security Manager must determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for incident response, risk assessments, emergency maintenance, and/or third-party audits. [AC-21 (a)]

To assist users in making information sharing and collaboration decisions, {Insert Company Name} employs access control, information flow monitoring (in accordance with the System and Communications Protection Policy and procedures), and media restrictions (in accordance with Media Protection Policy and procedures). [AC-21 (b)]

8.14 Publicly Accessible Information [AC-22]

{This section must be adjusted to meet your company’s policy} There is {no} publicly accessible information on the {Insert Product Name} Information System. {Describe the role or individuals authorized to post information on publicly accessible system}. [AC-22 (a)] {Describe the process if publicly accessible system content is reviewed for non-public information prior to posting}. [AC-22 (c)] As part of ongoing security awareness, the Information Security Team is responsible for training those individuals or groups responsible for reviewing all publicly accessible content. [AC-22 (b)]

The {Name company role or delegate who}, perform a quarterly review for non-public information. The following actions are taken during the quarterly review for non-public information: [AC-22 (d)]

* {Review of all public information systems that has been published}.
* {Documentation of all findings}.
* {Actions take to remediate sensitive content that is publicly accessible and who will do this action}.

9 Addendum A: List of Users Permitted to Access the Datacenter

In accordance with this policy, the following individuals (including employees, contractors, or vendors) are permitted to access the information datacenter locations without an escort:

|  |  |
| --- | --- |
| Name | Data Center Location |
|  |  |
|  |  |

10 ADDENDUM: List of Users with Remote Access Privileges

In accordance with this policy, the following individuals (including employees, contractors, or vendors) are permitted to remotely access the information system:

|  |  |  |
| --- | --- | --- |
| Name | Title/Job Role | Type of Method/Encryption |
|  | {Insert Information Security leadership role name} |  |
|  | Information System Security Manager |  |
|  | Senior ISSO |  |
|  | {Insert IT leadership role name} |  |
|  | IT Service Delivery Manager |  |
|  | System Administrator |  |
|  | Database Administrator |  |
|  | {Insert Name} Configuration Manager Administrator |  |
|  | Network Administrator |  |
|  | Security Analyst |  |

11 Addendum C: List of Users With Publicly Accessible Content Privileges

In accordance with this policy, the following individuals (including employees, contractors, or vendors) are permitted to post and manage the publicly accessible content of the information system:

|  |  |
| --- | --- |
| Name | Title/Job Role |
|  |  |

12 Addendum D: List of Current External Information Systems

In accordance with this policy, the following external information systems have been approved by the information Executive Management team for the information system:

|  |  |
| --- | --- |
| Name | Purpose |
| NIST NTP | Server clock time synchronization |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |