# Revision History and Approval

| Version | Date | Description |
| --- | --- | --- |
| 1.0 | 6/1/2020 | Inofrmation gathering |
| 2.0 | 2/5/2022 | General Update |
| 3.0 | 10/29/2023 | Security Categorization Review |
| 4.0 | 01/06/2024 | Risk Assessment, Contingency Plan Testing |

Prepared by:

| Identification of Organization that Prepared this Document | | |
| --- | --- | --- |
| Organization Name | Delojik Technology Academy |
| Street Address | Yaba Left, Lagos |
| Suite/Room/Building |  |
| City, State Zip | Lagos, Nigeria |

Prepared for:

| Identification of System Owner or Authorizing Official Organization | |
| --- | --- |
| Organization Name | Corporate Affairs Commision |
| Street Address | Wuse II |
| Suite/Room/Building |  |
| City, State Zip | Abuja, Nigeria |

This system security plan was approved by:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ISSO

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

System Owner

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CISO / ISSM

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorizing Official

**Table of Contents**

[1 Revision History and Approval ii](#_Toc346103316)

[2 Executive Summary 1](#_Toc346103317)

[2.1 Information System Name/Title 1](#_Toc346103318)

[2.2 Information System Categorization 1](#_Toc346103319)

[2.2.1 Information Types 1](#_Toc346103320)

[2.2.2 Security Objectives Categorization (FIPS 199) 3](#_Toc346103321)

[2.2.3 E-Authentication Determination (E-Auth) 3](#_Toc346103322)

[2.3 Information System Owner 5](#_Toc346103323)

[2.4 Authorizing Official 5](#_Toc346103324)

[2.5 Assignment of Security Responsibility 6](#_Toc346103325)

[2.6 Information System Operational Status 6](#_Toc346103326)

[2.7 Information System Type 7](#_Toc346103327)

[3 General System Description 7](#_Toc346103328)

[3.1 System Function or Purpose 7](#_Toc346103329)

[3.2 Information System Components and Boundaries 7](#_Toc346103330)

[3.3 Types of Users 7](#_Toc346103331)

[3.4 Network Architecture 8](#_Toc346103332)

[3.5 System Environment 8](#_Toc346103333)

[3.5.1 Hardware Inventory 8](#_Toc346103334)

[3.5.2 Software Inventory 8](#_Toc346103335)

[3.5.3 Network Inventory 9](#_Toc346103336)

[3.5.4 Data Flow 9](#_Toc346103337)

[3.5.5 Ports, Protocols and Services 9](#_Toc346103338)

[3.5.6 System Interconnections 10](#_Toc346103339)

[4 Applicable Laws and Regulations 10](#_Toc346103340)

[4.1 Applicable Laws 10](#_Toc346103341)

[4.2 NIH Policy, Guidance and Standards 11](#_Toc346103342)

[4.3 Applicable Federal Standards and Guidance 11](#_Toc346103343)

[5 Minimum Security Controls 12](#_Toc346103344)

[5.1 Control Selection and Implementation Status 12](#_Toc346103345)

[5.1.1 Control Type and Ownership Definitions 13](#_Toc346103346)

[5.1.2 NIST SP 800-53 Minimum Control Baseline with NIH Supplemental Controls 14](#_Toc346103347)

[5.1.3 Program Management Controls 14](#_Toc346103348)

[5.1.4 Industrial Control Systems Controls 15](#_Toc346103349)

[5.1.5 Trusted Internet Connection Controls 15](#_Toc346103350)

[5.1.6 NIH Supplemental Controls Part #1 15](#_Toc346103351)

[5.2 Control Implementation 16](#_Toc346103352)

[6 Appendix A: Glossary 18](#_Toc346103353)

[7 Appendix B: FIPS Pub 199 Categorization 19](#_Toc346103354)

[8 Appendix C: Privacy Threshold Analysis 20](#_Toc346103355)

[9 Appendix D: e-Authentication Risk Assessment 21](#_Toc346103356)

[10 Appendix E: Continuous Monitoring Strategy 22](#_Toc346103357)

# Executive Summary

This document details the System Security Plan (SSP) for the <Delojik Technology> security controls. This System Security Plan was written in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Revision 1, Guide for Developing Security Plans for Information Technology Systems. Completion of this SSP, which describes how U.S. federal information will be safeguarded, is a requirement of the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, the Computer Security Act of 1987, and NIH Cybersecurity Policy.

## Information System Name/Title

This System Security Plan provides an overview of the security requirements for the < Xoreta Academy system > (<**MLS>**) and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is an asset vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the < Medical Logistics System > information system.

The security safeguards implemented for the < Medical Logistics System > system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table : Information System Name and Title

|  |  |  |
| --- | --- | --- |
| Unique Identifier | Information System Name | Information System Abbreviation |
| 2857 | Delojik Technology System | DTS |

## Information System Categorization

### Information Types

This section describes how the information types used by the information system are categorized for confidentiality, integrity, and availability sensitivity levels.

The following tables identify the information types that are input, stored, processed, and/or output from < Medical Logistics System >. The selection of the information types is based on guidance provided by OMB Federal Enterprise Architecture Program Management Office Business Reference Model 2.0, and FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems* which is based on NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

The tables also identify the security impact levels for confidentiality, integrity, and availability for each of the information types expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity, and availability) discussed in NIST SP 800-60 and FIPS Pub 199.

The potential impact is *low* if—

- The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is *moderate* if—

- The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

- A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is *high* if—

- The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

- A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

**Note:** The information types found in NIST SP 800-60, Volumes I and II

Revision 1 is the same information types found in the Federal Enterprise Architecture (FEA) Consolidated Reference Model.

Table : Sensitivity Categorization of Information Types

| Information Type | Confidentiality | Integrity | Availability |
| --- | --- | --- | --- |
| Health Record | High | High | Low |
| Financial Data | Moderate | High | Low |
| Legal Cases | Moderate | Moderate | High |
| Training Records | Moderate | High | High |
| Contract | Moderate | High | Moderate |

### Security Objectives Categorization (FIPS 199)

Based on the information provided, Information Types, for the < Medical Logistics System > default to the high-water mark for the noted Information Types as identified in the table below.

Table : Security Impact Level

| Security Objective | Low, Moderate or High |
| --- | --- |
| Confidentiality | High |
| Integrity | High |
| Availability | High |
| Overall | High |

**Note:** Please refer to *FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems.*

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

### E-Authentication Determination (E-Auth)

E-Authentication applies to remote authentication of human users of Federal agency IT systems for the purposes of conducting government business electronically (or e-government). OMB M-04-04 and NIST SP 800-63 applies to all such transactions[[1]](#footnote-1) for which authentication is required, regardless of the constituency (e.g. individual user, business, or government entity).

Though authentication typically involves a computer or other electronic device, e-Authentication guidance (OMB M-04-04 and NIST SP 800-63) does not apply to the authentication of servers, or other machines and network components.

Each NIH system must be evaluated to determine whether e-authentication requirements apply. The table below provides the screening questions for making the initial applicability determination.

Table : E-Authentication Applicability Determination

|  |  |  |
| --- | --- | --- |
| Yes | No | E-Authentication Applicability Determination |
|  |  | Does the system require authentication via the Internet or other untrusted network? |
|  |  | Is data being transmitted over the Internet via browsers? |
|  |  | Do users connect to the system from over the Internet? |

If the responses to all questions above are YES, then the system is applicable to e-Authentication requirements and an e-Authentication Risk Assessment (eRA) is required.

**Note:** Please refer to *OMB Memo M-04-04 E-Authentication Guidance for*

*Federal Agencies* and NIST SP 800-63 for more information on e-Authentication.

*If the system is determined to be not applicable to e-Authentication, then specify N/A in the e-Authentication Assurance Level Determination below.*

For systems determined to be applicable to e-Authentication, an e-Authentication Risk Assessment must be performed in accordance OMB M-04-04 and NIST SP 800-63 guidelines. The result of that risk assessment is determination of the E-Authentication Assurance Level for the information system. The assurance level describes the System Owner’s degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as:

* The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and
* The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Table : e-Authentication Assurance Level

|  |  |  |
| --- | --- | --- |
| **e-Authentication Level** | **Maximum Impact Profile** | **Selection** |
| Not Applicable | None |  |
| Level 1: no identity proofing requirement | Low |  |
| Level 2: single factor remote authentication | Low |  |
| Level 3: multi-factor remote authentication | Moderate |  |
| Level 4: multi-factor remote authentication; hard crypto tokens | High |  |

The assurance level was determined through execution of the eRA. The NIH eRA tool compared the impact profile from the risk assessment to the impact profiles associated with each assurance level defined in OMB M-04-04. The assurance level was determined by identifying the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment. If the System Owner determined that mitigating circumstances or controls exist that permit a reduction of the derived assurance level, the justification was captured in the eRA.

*Note: The eRA may identify individual transactions that could be at different assurance levels within the same system. The System Owner may elect to define assurance level to the transaction level to better deploy cost effective and appropriate technical solutions specific to the assurance level of the transaction.*

## Information System Owner

The following individual is identified as the system owner or functional proponent/advocate for this system.

|  |  |
| --- | --- |
| Name | Samuel Esan |
| Title | ISO (Information System Owner) |
| Company / Organization | DTS |
| Address | Yaba, Lagos |
| Phone Number |  |
| Email Address | [Douglas.brain@nih.com](mailto:Douglas.brain@nih.com) |

## Authorizing Official

|  |  |
| --- | --- |
| Name | Karina Roach |
| Title | CIO (Chief Information Officer) |
| Company / Organization | XAS |
| Address |  |
| Phone Number |  |
| Email Address | [akinola.oluwole@nih.com](mailto:akinola.oluwole@nih.com) |

## Assignment of Security Responsibility

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

|  |  |
| --- | --- |
| Name | Samuel Esan |
| Title | ISSO |
| Company / Organization | Xoreta |
| Address | Houston, Texas |
| Phone Number |  |
| Email Address | Samuel.esan@xoreta.com |

## Information System Operational Status

The system is currently in the life-cycle phase noted in the table that follows.

| System Status | | |
| --- | --- | --- |
|  | Operational | The system is operating and in production. |
|  | Under Development | The system is being designed, developed, or implemented |
|  | Major Modification | The system is undergoing a major change, development, or transition. |
|  | Other | Explain: |

## Information System Type

| System Status | | |
| --- | --- | --- |
|  | General Support System |  |
|  | Major Application |  |
|  | Other | Explain: |

# General System Description

This section includes a general description of the <**Information System Name**>.

## System Function or Purpose

< This Information System primarily stores files and processes privacy (PII) data in the form of employee and patient health records, legal cases for NIH and training record of employees, as well as procurement information that includes contracts and financial data.

>

## Information System Components and Boundaries

<This section should include a description, in text, detailing the external boundaries of the information system. The description should address applicable environments other than the primary production environment (i.e maintenance, testing/development, or back-up environment).>

## Types of Users

All users have their employee status categorized with a sensitivity level in accordance with PS-2. Employees (or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in the table that follows.

| Role | Internal or External | Sensitivity Level | Authorized Privileges and Functions Performed |
| --- | --- | --- | --- |
| Standard User | Internal |  | Read Only Privilege |
| Super User | Internal |  | Read/write Privilege |
| Power User | Internal |  | Read/write/Execute privilege |

There are currently <**number**> of internal users and <**number**> of external users. Within one year, it is anticipated that there will be <**number**> of internal users and <**number**> of external users.

## Network Architecture

The following architectural diagram(s) provides a visual depiction of the major hardware components that constitute <**Medical Logistics System**>.

## System Environment

### Hardware Inventory

The following table lists the principal server hardware components for <**Medical Logistics System**>.

| Hostname/Name | **Make** | **Model and Firmware** | **Location** | **Components that Use this Device** |
| --- | --- | --- | --- | --- |
| Routers | Juniper |  | B 20 |  |
| Switches | Cisco |  |  |  |
| Work Stations | HP |  |  |  |
|  |  |  |  |  |

### Software Inventory

The following table lists the principal software components for **<**Information System Name**>**.

| Hostname/Name | Function | Version | Patch Level | Virtual (Yes / No) |
| --- | --- | --- | --- | --- |
| Intrusion Detection System |  |  |  |  |
| Active Directory |  | Widows 2008 |  |  |
| Apache |  | 2.0.64 & 2.2.15 |  |  |
| Weblogic |  | 103 |  |  |
| Oracle |  | 11g |  |  |

### Network Inventory

The following table lists the principle network devices and components for **<Medical Logistics System>**.

| Hostname | Make | Model | IP Address | Function |
| --- | --- | --- | --- | --- |
| Router | Juniper |  |  |  |
| Intrusion Detection System |  |  |  |  |
| Switches | Cisco |  |  |  |
| Firewall |  |  |  |  |

### Data Flow

<**insert diagram**>

### Ports, Protocols and Services

The table below lists the Ports, Protocols, and Services enabled in this information system. TCP ports are indicated with a T and UDP ports are indicated with a U.

| Ports (T or U) | Protocols | Services | Purpose | Used By |
| --- | --- | --- | --- | --- |
| 22 | SSH |  |  |  |
| 21 | FTP |  |  |  |
| 443 | Https |  |  |  |
| 53 | DNS |  |  |  |

### System Interconnections

| IP Address and Interface | External Organization Name and IP Address of System | Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer etc.) | Data Direction (incoming, outgoing, or both) | Ports or Circuit # |
| --- | --- | --- | --- | --- |
| 192.168.2.20/30 |  |  |  |  |
|  |  |  |  |  |

# Applicable Laws and Regulations

## Applicable Laws

The following laws and regulations apply to the information system:

* Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
* E-Authentication Guidance for Federal Agencies [OMB M-04-04]
* Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
* Freedom of Information Act As Amended in 2002 [PL 104-232, 5 USC 552]
* Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
* Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7]
* Internal Control Systems [OMB Circular A-123]
* Management of Federal Information Resources [OMB Circular A-130]
* Management’s Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
* Privacy Act of 1974 as amended [5 USC 552a]
* Protection of Sensitive Agency Information [OMB M-06-16]
* Records Management by Federal Agencies [44 USC 31]
* Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
* Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]

## NIH Policy, Guidance and Standards

The following standards and guidance apply to the information system:

* NIH Cybersecurity Policy, Order 1351.37, 2011
* NIH Cybersecurity Compendium, 2012
* NIH Security Authorization and Continuous Monitoring Performance Guide, 2012

## Applicable Federal Standards and Guidance

The following standards and guidance apply to the information system:

* Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
* Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Revision 1]
* Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]
* Guide for Mapping Types of Information and Information Systems to Security Categories [NISP SP 800-60, Revision 1]
* Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
* Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
* Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 4]
* Risk Management Guide for Information Technology Systems [NIST SP 800-30]
* Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
* Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]

**Note:** All NIST Computer Security Publications can be found at the following

URL: <http://csrc.nist.gov/publications/PubsSPs.html>

# Minimum Security Controls

Security controls must meet minimum security control baseline requirements. There are security control baseline requirements for management controls, operational controls, and technical controls.

Management security controls identify the management safeguards and countermeasures in-place or planned for <**Medical Logistics System**>. Management Controls are those safeguards and countermeasures that focus on the management of risk and the management of the information security system. They are actions that are performed primarily to support information system security management decisions. Operational security controls identify the operational safeguards and countermeasures in-place or planned for <**Medical Logistics System**>. Operational controls are those safeguards and countermeasures that are primarily implemented and executed by people as opposed to systems and technology. Technical security controls identify the technical safeguards and countermeasures in-place or planned for <**Medical Logistics System**>. Technical Controls are those safeguards and countermeasures that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

5.1. **Access control (AC)**

|  |  |  |
| --- | --- | --- |
| AC-6 | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned * Not Applicable |  | |
| Control Type: |  | |
|  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | |  | | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned * N/A * Inherited |  | |
| Control Type |  | |
|  | | |

|  |  |  |
| --- | --- | --- |
| AC-2(1) | | AUTOMATED SYSTEM ACCOUNT MANAGEMENT |
| **Support the management of system accounts using [*Assignment: organization-defined automated mechanisms*].** | | |
| Implementation Status  * Implemented * Not Implemented * Planned * Inherited | Implemented | |
| Control Type: | Hybrisd | |
| Implementation Statement | | |

|  |  |  |
| --- | --- | --- |
| AC - 4 | | **INFORMATION FLOW ENFORCEMENT** |
| The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [*Assignment: organization-defined information flow control policies*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AC-5 | | **SEPARATION OF DUTIES** |
| The organization:  a. Separates [*Assignment: organization-defined duties of individuals*];  b. Documents separation of duties of individuals; and  c. Defines information system access authorizations to support separation of duties. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AC-6 | | **LEAST PRIVILEGE** |
| The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AC-7 | | **UNSUCCESSFUL LOGON ATTEMPTS** |
| The information system:  a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*]; and  b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next logon prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AC-8 | | **SYSTEM USE NOTIFICATION** |
| The information system:  a. Displays to users [*Assignment: organization-defined system use notification message or banner*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:  1. Users are accessing a U.S. Government information system;  2. Information system usage may be monitored, recorded, and subject to audit;  3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and  4. Use of the information system indicates consent to monitoring and recording;  b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and  c. For publicly accessible systems:  1. Displays system use information [*Assignment: organization-defined conditions*], before granting further access;  2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such  systems that generally prohibit those activities; and  3. Includes a description of the authorized uses of the system. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AC-11 | | **SESSION LOCK** |
| The information system:  a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and  b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AC-12 | | **SESSION TERMINATION** |
| The information system automatically terminates a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AC-14 | | **PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION** |
| The organization:   1. Identifies [*Assignment: organization-defined user actions*] that can be performed on the information system without   identification or authentication consistent with organizational missions/business functions; and   1. Documents and provides supporting rationale in the security plan for the information system, user actions not   requiring identification or authentication. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AC-17 | | **REMOTE ACCESS** |
| The organization:   1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance   for each type of remote access allowed; and  b. Authorizes remote access to the information system prior to allowing such connections. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AC-18 | | **WIRELESS ACCESS** |
| The organization:   1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless   access; and  b. Authorizes wireless access to the information system prior to allowing such connections. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AC-19 | | **ACCESS CONTROL FOR MOBILE DEVICES** |
| The organization:   1. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance   for organization-controlled mobile devices; and  b. Authorizes the connection of mobile devices to organizational information systems. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AC-21 | | **INFORMATION SHARING** |
| The organization:  a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and  b. Employs [*Assignment: organization-defined automated mechanisms or manual processes*] to assist users in making information sharing/collaboration decisions. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| IA-2 | | **IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)** |
| The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| IA-3 | | **DEVICE IDENTIFICATION AND AUTHENTICATION** |
| The information system uniquely identifies and authenticates [*Assignment: organization-defined specific and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| IA-4 | | **IDENTIFIER MANAGEMENT** |
| The organization manages information system identifiers by:  a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier;  b. Selecting an identifier that identifies an individual, group, role, or device;  c. Assigning the identifier to the intended individual, group, role, or device;  d. Preventing reuse of identifiers for [*Assignment: organization-defined time period*]; and  e. Disabling the identifier after [*Assignment: organization-defined time period of inactivity*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| IA-5 | | **AUTHENTICATOR MANAGEMENT** |
| The organization manages information system authenticators by:  a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;  b. Establishing initial authenticator content for authenticators defined by the organization;  c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;  d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;  e. Changing default content of authenticators prior to information system installation;  f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;  g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*];  h. Protecting authenticator content from unauthorized disclosure and modification;  i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and  j. Changing authenticators for group/role accounts when membership to those accounts changes. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| IA-6 | | **AUTHENTICATOR FEEDBACK** |
| The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| IA-7 | | **CRYPTOGRAPHIC MODULE AUTHENTICATION** |
| The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| IA-8 | | **IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)** |
| The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AT-1 | | **SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES** |
| The organization:  a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:  1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and  b. Reviews and updates the current:  1. Security awareness and training policy [*Assignment: organization-defined frequency*]; and  2. Security awareness and training procedures [*Assignment: organization-defined frequency*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AT-2 | | **SECURITY AWARENESS TRAINING** |
| The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):  a. As part of initial training for new users;  b. When required by information system changes; and  c. [*Assignment: organization-defined frequency*] thereafter. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AT-3 | | **ROLE-BASED SECURITY TRAINING** |
| The organization provides role-based security training to personnel with assigned security roles and responsibilities:  a. Before authorizing access to the information system or performing assigned duties;  b. When required by information system changes; and  c. [*Assignment: organization-defined frequency*] thereafter. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AT-4 | | **SECURITY TRAINING RECORDS** |
| The organization:  a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and  b. Retains individual training records for [*Assignment: organization-defined time period*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AU-1 | | **AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES** |
| The organization:  a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:  1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and  b. Reviews and updates the current:  1. Audit and accountability policy [*Assignment: organization-defined frequency*]; and  2. Audit and accountability procedures [*Assignment: organization-defined frequency*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AU-2 | | **AUDIT EVENTS** |
| The organization:  a. Determines that the information system is capable of auditing the following events: [*Assignment: organization-defined auditable events*];  b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;  c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and  d. Determines that the following events are to be audited within the information system: [*Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AU-3 | | **CONTENT OF AUDIT RECORDS** |
| The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AU-4 | | **AUDIT STORAGE CAPACITY** |
| The organization allocates audit record storage capacity in accordance with [*Assignment: organization-defined audit record storage requirements*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AU-5 | | **RESPONSE TO AUDIT PROCESSING FAILURES** |
| The information system:  a. Alerts [*Assignment: organization-defined personnel or roles*] in the event of an audit processing failure; and  b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information*  *system, overwrite oldest audit records, stop generating audit records)*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AU-8 | | **TIME STAMPS** |
| The information system:  a. Uses internal system clocks to generate time stamps for audit records; and  b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*Assignment: organization-defined granularity of time measurement*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AU-9 | | **PROTECTION OF AUDIT INFORMATION** |
| The information system protects audit information and audit tools from unauthorized access, modification, and deletion. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| AU-11 | | **AUDIT RECORD RETENTION** |
| The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| CA-1 | | **SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES** |
| The organization:  a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:  1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and  b. Reviews and updates the current:  1. Security assessment and authorization policy [*Assignment: organization-defined frequency*]; and  2. Security assessment and authorization procedures [*Assignment: organization-defined frequency*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| CA-2 | | **SECURITY ASSESSMENTS** |
| The organization:  a. Develops a security assessment plan that describes the scope of the assessment including:  1. Security controls and control enhancements under assessment;  2. Assessment procedures to be used to determine security control effectiveness; and  3. Assessment environment, assessment team, and assessment roles and responsibilities;  b. Assesses the security controls in the information system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;  c. Produces a security assessment report that documents the results of the assessment; and  d. Provides the results of the security control assessment to [*Assignment: organization-defined individuals or roles*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| CA-3 | | **SYSTEM INTERCONNECTIONS** |
| The organization:   1. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; 2. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the   information communicated; and  c. Reviews and updates Interconnection Security Agreements [*Assignment: organization-defined frequency*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| CA-4 | | **SECURITY CERTIFICATION** |
| [Withdrawn: Incorporated into CA-2]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| CA-5 | | **PLAN OF ACTION AND MILESTONES** |
| The organization:  a. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and  b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| CA-6 | | **SECURITY AUTHORIZATION** |
| The organization:  a. Assigns a senior-level executive or manager as the authorizing official for the information system;  b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and  c. Updates the security authorization [*Assignment: organization-defined frequency*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| CA-7 | | **CONTINUOUS MONITORING** |
| The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:  a. Establishment of [*Assignment: organization-defined metrics*] to be monitored;  b. Establishment of [*Assignment: organization-defined freq*uencies] for monitoring and [*Assignment: organization-defined freq*uencies] for assessments supporting such monitoring;  c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;  d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;  e. Correlation and analysis of security-related information generated by assessments and monitoring;  f. Response actions to address results of the analysis of security-related information; and  g. Reporting the security status of organization and the information system to [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| CM-1 | | **CONFIGURATION MANAGEMENT POLICY AND PROCEDURES** |
| The organization:  a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:  1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and  b. Reviews and updates the current:  1. Configuration management policy [*Assignment: organization-defined frequency*]; and  2. Configuration management procedures [*Assignment: organization-defined frequency*]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| CM-2 | | **BASELINE CONFIGURATION** |
| The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
| CM-3 | | **CONFIGURATION CHANGE CONTROL** |
| The organization:  a. Determines the types of changes to the information system that are configuration-controlled;  b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;  c. Documents configuration change decisions associated with the information system;  d. Implements approved configuration-controlled changes to the information system;  e. Retains records of configuration-controlled changes to the information system for [*Assignment: organization-defined time period*];  f. Audits and reviews activities associated with configuration-controlled changes to the information system; and  g. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board)*] that convenes [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]]. | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | | |
| Implementation Status  * Implemented * Not Implemented * Planned |  | |
| Responsible Roles: |  | |
| Implementation Details: The IT security Policy document has been developed and disseminated to all system users. It provides the governance for IT standards which address scope, roles, responsibilities, management, and coordination among various organization entities. | | |

1. For the purposes of e-Authentication, a transaction is defined as: a discrete event between a user and systems that supports a business or programmatic purpose. [↑](#footnote-ref-1)