<TEMPLATE>

System Security Plan

<AGENCY>

<System Name>

<Plan Version 2.0>

<Date>

TABLE OF CONTENTS

[Document Revision History 3](#_Toc158388532)

[Prepared by 3](#_Toc158388533)

[Prepared for 3](#_Toc158388534)

[1. SYSTEM SECURITY PLAN APPROVALS 4](#_Toc158388535)

[2. EXECUTIVE SUMMARY 5](#_Toc158388536)

[3. SYSTEM INFORMATION 6](#_Toc158388537)

[**3.1 System Definition: Key attributes of the System / Cloud Service Offering (CSO)** 6](#_Toc158388538)

[4. CONTACT INFORMATION 8](#_Toc158388539)

[**4.1 Authorizing Official** 8](#_Toc158388540)

[**4.2 System Owner** 8](#_Toc158388541)

[**4.3 Information Owner (A.K.A. Data Owner)** 9](#_Toc158388542)

[**4.4 Assignment of Security Responsibility: Agency Chief Information Security Officer / Information Security Officer** 10](#_Toc158388543)

[5. SYSTEM ADMINISTRATION 10](#_Toc158388544)

[6. Technical System Information 11](#_Toc158388545)

[**6.1 Type of Users** 11](#_Toc158388546)

[**6.2 Software Inventory** 11](#_Toc158388547)

[**6.3 Remote Services (Other Than Web Services / Cloud)** 12](#_Toc158388548)

[**6.4 Security and Management Technologies** 12](#_Toc158388549)

[7. Illustrated Architecture and Narratives 13](#_Toc158388550)

[**7.1 Illustrated Architecture** 13](#_Toc158388551)

[**7.2 System/Authorization Boundary Diagram** 14](#_Toc158388552)

[**7.3 Network Diagram** 15](#_Toc158388553)

[**7.4 Information/Data Flow Diagram** 15](#_Toc158388554)

[8. Services, Ports, and Protocols 16](#_Toc158388555)

[9. Separation of Duties 17](#_Toc158388556)

[10. System Interconnections / External Systems and Services 18](#_Toc158388557)

[11. Minimum Security Controls 24](#_Toc158388558)

[SSP Required Appendices List 227](#_Toc158388559)

# **Document Revision History**

| **Date** | **Description** | **Version** | **Author** |
| --- | --- | --- | --- |
| 02/05/2024 | Initial publication for GTA SSP Template at 800-53 Rev.5 | Plan 2.0 | GTA OIS |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

# **Prepared by**

|  |  |
| --- | --- |
| Identification of Organization, Vendor that Prepared this Document | |
| **Organization Name** | <Enter Company/Organization> |
| **Street Address** | <Enter Street Address> |
| **Suite/Room/Building** | <Enter Suite/Room/Building> |
| **City, State, Zip** | <Enter City, State, and Zip Code> |

# **Prepared for**

|  |  |
| --- | --- |
| Identification of Cloud Service Provider | |
| **Organization Name** | <Enter Company/Organization>. |
| **Street Address** | <Enter Street Address> |
| **Suite/Room/Building** | <Enter Suite/Room/Building> |
| **City, State, Zip** | <Enter City, State, and Zip Code> |
|  |  |

# **1. SYSTEM SECURITY PLAN APPROVALS**

|  |
| --- |
| ***Instructions:*** |
| *Add or remove signature boxes, as needed. Digital or wet/physical signatures are permitted.* |

**Authorized by Signatures**

By signing this System Security Plan (SSP), we agree that it is complete and is the current version to be used for the security assessment.

**System Owner**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| <Sign Here> | | | | |
| Name | <Enter Name> | | Date | <Date> |
| Title | <Enter Title> | | | |
| Agency | | <Name> | | |
|  | | | | |
| **Agency CISO / ISO** | | | | |
| <Sign Here> | | | | |
| Name | <Enter Name> | | Date | <Date> |
| Title | <Enter Title> | | | |
| Agency | | <Name> | | |
|  | | | | |
| **Agency Head or Authorizing Official** | | | | |
| <Sign Here> | | | | |
| Name | <Enter Name> | | Date | <Date> |
| Title | <Enter Title> | | | |
| Agency | | <Name> | | |
|  | |  | | |

# **2. EXECUTIVE SUMMARY**

[Provide a high-level executive summary of the system security plan]

Describe the system, environment, work you have done regarding the system implementation for the environment; relevant findings and relevant aspects to consider such as being in compliance with HIPAA, etc.

Provide a brief explanation of the business benefit, the importance of this system and what the system delivers and the main purpose/intentions of this SSP.

*{A summary table is provided for the Executive review. Although not required, it is recommended as an overview of the control implementation status for each control family.}*

**Controls Status Summary Table**

| **Control Family** | **In Place** | **Partially In Place** | **Not In Place** | **Not Applicable** |
| --- | --- | --- | --- | --- |
| Access Control (xx applicable number of controls) | 1 | 1 | 0 | 0 |
| Awareness and Training | 0 | 0 | 0 | 0 |
| Audit and Accountability | 0 | 0 | 0 | 0 |
| Assessment, Authorization, and Monitoring | 0 | 0 | 0 | 0 |
| Configuration Management | 0 | 0 | 0 | 0 |
| Contingency Planning | 0 | 0 | 0 | 0 |
| Identification and Authentication | 0 | 0 | 0 | 0 |
| Incident Response | 0 | 0 | 0 | 0 |
| Maintenance | 0 | 0 | 0 | 0 |
| Media Protection | 0 | 0 | 0 | 0 |
| Physical and Environmental Protection | 0 | 0 | 0 | 0 |
| Planning | 0 | 0 | 0 | 0 |
| Personnel Security | 0 | 0 | 0 | 0 |
| Risk Assessment | 0 | 0 | 0 | 0 |
| System and Services Acquisition | 0 | 0 | 0 | 0 |
| System and Communications Protection | 0 | 0 | 0 | 0 |
| System and Information Integrity | 0 | 0 | 0 | 0 |
| Supply Chain Risk Management | 0 | 0 | 0 | 0 |
| **Totals** | 0 | 0 | 0 | **0** |

# **3. SYSTEM INFORMATION**

The following subsections provide a description of services, functions, environment, and the personnel responsible for its security and management.

## **3.1 System Definition: Key attributes of the System / Cloud Service Offering (CSO)**

|  |
| --- |
| ***Instructions:*** |
| *Complete Table 3.1 as indicated. The FIPS PUB 199 Level should be completed after completing the corresponding appendices and determining appropriate content.*   * ***Fully Operational as of:*** *“Fully operational” means there are no “gaps” in the security control baseline implementations for the system.* * ***System Categorization: FIPS 199 Categorization / Data Set Categorization.***   ***\*\* [Attach FIPS 199 Worksheet (risk, information types, security impact levels) to the SSP*** ***Appendix K or insert file object here].***   * + *Identify Information Type* and *the security impact levels for confidentiality, integrity, and availability for each of the information types expressed as low, moderate, or high. (Use only information types that are input, stored, processed and/or output from Information System). Default to the high-water mark for the Information* *Types as identified in Security Impact Level.*   *The selection of the information types is based on guidance provided FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems which is based on NIST Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories. Consider the data sensitivity and system mission criticality to determine the potential impact that would be caused by a loss of confidentiality, integrity, or availability of the information system and/or its data.*   * + *Work with the Agency CISO/ISO, Authorizing Official, System Owner, Information Owner to rate the potential impact to the business or system in the event of unauthorized disclosure, modification, or unavailability of this information and/or information system.* * ***System Description****: Provide a description of all services and features that are included as part of this System / CSO and within the authorization boundary. The description should only include those items inside the service boundary that have been independent assessor (IA) tested as part of this assessment.* * *A service description should incorporate the purpose and functional characteristics of a system / CSO.* * *A service description should not include marketing language and is not meant to be a place where a company should be promoting or showcasing company accomplishments.* * *A service description should provide a representation of the services, features or components that have been tested and accredited as part of a CSO’s authorization boundary.* * *A service description should note the intended user base specifics for Hybrid and Government-only Community Cloud CSOs.*   Delete this and all other instructional text from your final version of this document. |

|  |  |
| --- | --- |
| System Information | |
| **Cloud Service Provider (CSP) Name:** | <Insert CSP Name> <Insert CSP Abbreviation, as appropriate> |
| **System / Cloud Service Offering (CSO) Name:** | <Insert CSO Name> <Insert CSO Abbreviation, as appropriate> |
| **Service Model:** | <Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS> |
| **Information System Categorization: FIPS Publication 199 (SSP Appendix K):** | <Choose one: High, Moderate, Low, LI-SaaS>  **[Attach** **System FIPS 199 Categorization Worksheet (risk, information types, security impact levels) to the SSP Appendix K or insert file object here].** |
| **Fully Operational as of:** | <Insert MM/DD/YYYY> |
| **System Description:** | <Insert System / CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)]. |
| **Regulatory Compliance** | <Choose applicable: HIPAA, PCI-DSS, FTI (IRS1075), FISMA, SSA, CJIS, CMS, Other regulatory \_\_\_\_> |

# **4. CONTACT INFORMATION**

## **4.1 Authorizing Official**

The following individual is identified as the Authorizing Official. The authorizing official (or designated approving/accrediting authority as referred to by some agencies) is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. The authorizing official has the following responsibilities related to system security plans:

* Approves system security plans,
* Authorizes operation of an information system,
* Issues an interim authorization to operate the information system under specific terms and conditions, or
* Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist. The Authorizing Official is responsible for approving the security implementation of the system.

| **Authorizing Official** | |
| --- | --- |
| **Name** | <Enter Name> |
| **Title** | <Enter Title> |
| **Agency / Office Designation** | <Enter Company/Organization> |
| **Address** | <Enter Address, City, State and Zip> |
| **Phone Number** | <555-555-5555> |
| **Email Address** | <Enter email address> |

## **4.2 System Owner**

The following individual is identified as the system owner or functional proponent/advocate for this system. The system owner is the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the system. The system owner has the following responsibilities related to system security plans:

* Develops the system security plan in coordination with information owners, the system administrator, and functional "end users,"
* Maintains the system security plan and ensures that the system is deployed and operated according to the agreed-upon security requirements,
* Ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior),
* Updates the system security plan whenever a significant change occurs, and
* Assists in the identification, implementation, and assessment of common security controls.

| System Owner Information | |
| --- | --- |
| **Name** | <Enter Name> |
| **Title** | <Enter Title> |
| **Agency / Office Designation** | <Enter Agency> |
| **Address** | <Enter Address, City, State and Zip> |
| **Phone Number** | <555-555-5555> |
| **Email Address** | <Enter Email Address> |

## **4.3 Information Owner (A.K.A. Data Owner)**

The following individual is identified as the Information Owner. The Information Owner is the agency official with the statutory or operational authority for the information processed, stored, or transmitted as part of this system and/or its functions and operation. The information owner has the following responsibilities related to system security plans:

* Establishes the rules for appropriate use and protection of the subject data/information (rules of behavior),
* Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information resides,
* Decides who has access to the information system and with what types of privileges or access rights, and
* Assists in the identification and assessment of the common security controls where the information resides.

| **Information Owner** | |
| --- | --- |
| **Name** | <Enter Name> |
| **Title** | <Enter Title> |
| **Agency / Office Designation** | <Enter Company/Organization> |
| **Address** | <Enter Address, City, State and Zip> |
| **Phone Number** | <555-555-5555> |
| **Email Address** | <Enter email address> |

## **4.4 Assignment of Security Responsibility: Agency Chief Information Security Officer / Information Security Officer**

The following individual is identified as the Agency Chief Information Security Officer / Information Security Officer assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

| **Agency Chief Information Security Officer (CISO) / Information Security Officer (ISO)** | |
| --- | --- |
| **Name** | <Enter Name> |
| **Title** | <Enter Title> |
| **Agency / Office Designation** | <Enter Company/Organization> |
| **Address** | <Enter Address, City, State and Zip> |
| **Phone Number** | <555-555-5555> |
| **Email Address** | <Enter email address> |

# 

# **5. SYSTEM ADMINISTRATION**

This system is managed by [*both External Support Team (EST) and the <ORGANIZATION> Team*]. List the Agency Administrators and the [*EST Administrators*]. Additionally list all groups, or individuals not in groups, that have administrative access to the system or its application.

| **Groups/Individuals, if possible, responsible for administrative functions of the** **System/CSP/CSO** |
| --- |
| * **Group Name** * **Name** * **Name** |

# **6. Technical System Information**

## **6.1 Type of Users**

Employees (or contractors) of [AGENCY] 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** | **Authorized Privileges and Functions Performed** | **Approximate # of users** |
| --- | --- | --- | --- |
| Admins | Internal | Admin | 5 |
| Users | Internal/External | User | 100 |
|  |  |  |  |

## **6.2 Software Inventory**

The following table lists the principal software components for <**System/CSO name**>**.**

| **Hostname** | **Function** | **Version** | **Patch Level** | **IP Address** | **Virtual (Yes / No)** |
| --- | --- | --- | --- | --- | --- |
| *i.e. <system name> state of georgia.gov* | *Operating System* | *Windows Server 2012 R2* | *Service Pack 1* | *255.255.255.255* | *Yes* |
|  |  |  |  |  |  |

## **6.3 Remote Services (Other Than Web Services / Cloud)**

Will users, contractors, administrators, vendors connect to the system using any of the following services?

|  |  |  |  |
| --- | --- | --- | --- |
| **Remote Management Services Questions** | | | |
|  | FTP |  | VNC |
|  | SFTP |  | RDP |
|  | Telnet |  | Citrix |
|  | SSH |  | Other: Click here to enter text. |

## **6.4 Security and Management Technologies**

|  |  |
| --- | --- |
| Category | Technical Solution / Vendor |
| Operating Systems |  |
| IAM/Access Management |  |
| Endpoint/Antivirus (AV), File Integrity Monitoring (FIM) |  |
| Configuration Management |  |
| Firewall/VPN |  |
| MFA |  |
| SIEM |  |
| Secrets Management |  |
| Vulnerability Scanning |  |

# **7. Illustrated Architecture and Narratives**

|  |
| --- |
| ***Instructions:*** |
| *Ensure the inventory items are named consistently, within the diagrams and within the narratives, in the sections that follow. Ensure naming conventions are adopted throughout the entire SSP (i.e., security control implementation descriptions and all attachments).*  *Delete this and all other instructional text from your final version of this document.* |

This section contains the diagrams and narratives for the <Insert System/CSO Name> authorization boundary, network, and data flows. Section 7.1 provides the diagrams, and Section 7.2 provides the associated narratives.

## **7.1 Illustrated Architecture**

|  |
| --- |
| ***Instructions:*** |
| *In this section, provide the illustration(s) for the System/CSO’s authorization boundary, network architecture, and data flows. The illustration can be one all-encompassing diagram that addresses all required informational elements, or separate diagrams (System/Authorization Boundary Diagram [ABD], Network Diagram, Data Flow Diagram [DFD]) if there is concern about too much data on one diagram; however, if more than one diagram is used,* ***ALL diagrams must be consistent (using same component names, color coding, etc.) and represent at least the authorization boundary and its components****.*  ***NARRATIVE DESCRIPTION for the ABD, DFD, and Network Diagram:***  *Whether using one or multiple diagrams, after each, provide a detailed narrative description that clearly describes the System/CSO and the elements of the diagram. The narrative should describe the components of the system as depicted in the diagram using the same naming conventions, to avoid confusion. Additionally, the narrative must describe the relationships of the internal services. It may be useful to describe these using a numbering or lettering scheme and then include them in the diagram (i.e., enabling the narrative to act as a key for the diagram). Ensure to reference the diagram(s) by figure number in the narrative description, and name the diagram appropriately. If you choose to have separate diagrams, ensure that there is an appropriate narrative provided for each diagram.*  *Choose the appropriate paragraph based on the number of diagrams; delete the other.*  *Delete this and all other instructional text from your final version of this document.* |

This section contains the diagram that represents the authorization boundary, network, and data flows. Following the diagram, there is a narrative that describes the <Insert System/CSO Name> boundary components, functionality, as well as interactions and flows among internal components and external systems/services.

or

This section contains the diagrams that represent the authorization boundary, network, and data flows. Following each of the diagrams, there is a narrative that describes the <Insert System/CSO Name> boundary components, functionality, as well as interactions and flows among internal components and external systems/services. If using several illustrations, each must have a narrative.

## **7.2 System/Authorization Boundary Diagram**

|  |
| --- |
| ***Instructions:*** |
| ***System/Authorization Boundary Diagram****:*  *An acceptable ABD has a clearly marked boundary. Include a prominent border (e.g., a bold red line) around all systems and services included in the authorization boundary. The diagram must be legible and readable. Please note that some authorization boundary diagrams are large once all the required data and information has been included.*  *The diagram(s) should:*   * *Include a clearly defined authorization boundary (e.g. bold red line).* * *Include system interconnections used to operate and support the intended mission/business functions.* * *Depict every tool, service, or component that is mentioned in the SSP narrative and controls.* * *Identify those depicted tools, services, or components as either external or internal to the boundary.* * *Clearly identify anywhere State data is to be processed, stored, or transmitted.* * *Depict how the CSP and customer/agency access the service (e.g., the authentication used to access the service).* * *Depict all major software/virtual components (or groups of) within the boundary.* * *Depict all CSP-provided components that are deployed in customer environments that are within the boundary.* * *Be validated against the inventory.*   + *Component labels on diagrams should match corresponding entries in the "Diagram Label" column in the inventory workbook.*   + *The “Function” column in the inventory workbook should describe the function performed by the component within the CSO.*   + *All components internal to the CSO should appear both in the inventory and on the diagrams.*   + *It is understood that a single component on a diagram may represent many entries in the inventory.* * *Show an alternate processing site.* * *Show how updates are pulled from external services (e.g., the operating system (OS), antivirus software, etc.).*   *Delete this and all other instructional text from your final version of this document.* |

*< Provide diagram of System/Authorization Network>*

## **7.3 Network Diagram**

|  |
| --- |
| ***Instructions:*** |
| ***Network Diagram:***  *If using a separate network overlay diagram, this should resemble the ABD and should include:*   * *Subnetworks* * *Location of DNS authoritative and recursive servers*   *Delete this and all other instructional text from your final version of this document.* |

*< Provide diagram of Network>*

## **7.4 Information/Data Flow Diagram**

|  |
| --- |
| ***Instructions:*** |
| ***Information/Data Flow Diagram:***  *If using a separate data flow overlay diagram, this should resemble the ABD, include the network components, and:*   * *Clearly identify data flows for privileged, non-privileged, and customers' access with MFA details.* * *Depict how all ports, protocols, and services of all internal and external traffic are represented and managed.* * *For each data flow, clearly depict protective mechanisms (i.e., the encryption type and FIPS 140-validation or use of other alternative implementations such as physical protection via protective distribution systems [PDS]), where applicable).* * *For each data store, clearly depict the encryption status (i.e., encrypted with FIPS 140 validated crypto modules, encrypted without FIPS, or unencrypted).The best approach is to use the reference # from the encryption tables below.*   *Delete this and all other instructional text from your final version of this document.* |

*<Insert Data Flow Diagram>*

# **8. Services, Ports, and Protocols**

Table 9.1 lists the service names, port numbers, and transport protocols enabled in <Insert System/CSO Name>. These must be specifically called out per the security control requirements in CM-7, CM-7(1), RA-5, SA-4, SA-9(2), and SA-9(4).

|  |
| --- |
| ***Instructions:*** |
| ***Complete this table even if leveraging a pre-existing authorization.*** *Add more rows as needed. If you are unclear as to what should be included in this table, refer to:* <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>.  *Ensure that the services, ports, and protocols match the data collected in the rest of this SSP.*  *The developer of the system, system component, or system service is required to identify the functions, ports, protocols, and services intended for organizational use. This list must be kept current. It becomes resource-intensive to retrofit security controls after the system, component, or service has been implemented.*  ***Reference #:*** *Match this number to the reference number (“Ref #”) column in Appendix Q.*  ***Purpose:*** *Provide a general description of how it is used in the CSO, such as for Web access or database connection.*  ***Used By:*** *List the CSO components accessed by this port and the stated purpose.*  Delete this and all other instructional text from your final version of this document. |

# **9. Separation of Duties**

Security control AC-5, Separation of Duties, requires the identification and documentation for roles of ***all*** individuals who access the system and define the access authorizations that support protections from bad actors, employee collusion, fraud, etc. before damage occurs. Table 11.1 captures the roles and access privileges for all individuals or roles that access <Insert System/CSO Name>.

|  |
| --- |
| ***Instructions:*** |
| *In Table 11.1, identify and document all duty descriptions within the organization. Each duty description is listed in a separate row; if a CSP is a large and complex organization, there could be several. In the case of a CSP being large and complex, focus on the duty descriptions that apply to the System/CSO. There may be third party relationships that apply such as administrators who are not part of the organization; these should also be listed. Additionally, the table should include any duties performed by agency customers. Table 11.1 includes a few examples, which should be removed prior to populating this table for your System/CSO.*  *Identify and document all general roles for the organization or the System/CSO (one for each column); there may be indirect roles that apply that should also be listed.*  *If the System/CSO has many more duties and roles than what can fit within a table of this size, you may use an Excel spreadsheet and reference it as an appendix within the SSP and this section.*  *Delete this and all other instructional text from your final version of this document.* |

| Duty Description | Information Owner | Security officer | Privacy officer | Linux Admin | Windows Admin | Agency Admin |
| --- | --- | --- | --- | --- | --- | --- |
| Adds/Removes Privileged Admins | X | X |  |  |  |  |
| Adds/Removes Non-privileged Admins |  | X | X |  |  |  |
| Adds/Removes Customer Privileged Admins |  |  |  |  |  |  |
| Adds/Removes Customer Non-Privileged Admins |  |  |  |  |  |  |
| Enforces Physical Access Authorizations |  |  |  |  |  |  |
| Defines Least Privilege Needed to Perform Tasks |  |  |  |  |  |  |
| Reviews/Approves Policy |  |  |  |  |  |  |
| Enforces Policy |  |  |  |  |  |  |

# **10. System Interconnections / External Systems and Services**

|  |
| --- |
| ***Instructions:*** |
| *Populate the columns as follows:*  ***System/Service/API/CLI Name (Non-FedRAMP Cloud Services)****: Provide the name of the system, service, API, or CLI. Include the vendor name, if different from the product name.*  ***Connection Details:*** *Provide connectivity details. Specifically, note data direction whether inbound, outbound, or both. Connection security (VPN, SSL< Certificates, SFT, etc.)*  ***Nature of Agreement and Date of Agreement****: The "Nature of Agreement" is any type of agreement between the CSP and the leveraged CSP vendors who support products (e.g., End User Licensing Agreement (EULA), Service-Level Agreement (SLA), App License Agreement, Contract, etc.).*  ***Still supported? Y or N****: Is this product still supported by the manufacturer?*  ***Data Types****: List the data types and metadata types transmitted to, stored, or processed by the system/service, including federal data and sensitive system data. This column is based on the NIST 800-60 Vol. II data types for the system. Longer lists of data types and data categorizations may instead be included in an appendix.*  ***Data Categorization****: Identify the security impact level of the data (Low, Moderate, High) in accordance with FIPS 199 & NIST 800-60 Vol. 2. Longer lists of data types and data categorizations may instead be included in an appendix.*  ***Authorized Users/Authentication****: List the user roles (e.g., SecOps engineers) authorized to access the service, and provide the authentication method.*  ***Other Compliance Programs****: List any certifications for this service (e.g., PCI SOC 2, CSA STAR Level 2, etc.), and provide the certification date. If FISMA is authorized, that should also be specifically noted.*  ***Description****: Describe the purpose of the Interconnected system, external system/service; specifically, provide reasons for connectivity (e.g., system monitoring, system alerting, download updates, etc.).*  ***Hosting Environment****: Describe the hosting environment (e.g., corporate network, IaaS, or self-hosted).*  ***Risk/Impact/ Mitigation****: Describe potential risks introduced by the external system/service and impact to the CSO or federal data if the CIA of the system/service is compromised. Describe any mitigations or compensating controls in place to reduce risk.*  *Delete this and all other instructional text from your final version of this document.* |

System Interconnections / Information Sharing, External Systems/Services, APIs, and CLIs

| System/ Service/ API/CLI Name (Non-FedRAMP Cloud Services) | Organization / Agency | Connection Details | Nature of Agreement and Date (ISA/MOU/OU ; Date of agreement to interconnect) | Still Supported? Y or N | Data Types | Data Categorization (FIPS199 Categorization) | Authorized Users/ Authentication | Other Compliance Programs | Description | Hosting Environment | Risk/Impact/ Mitigation | Authorizing Official |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

# **11. Minimum Security Controls**

**Access Control**

**AC-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] access control policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **AC-1 Control Summary Information** |
| Responsible Role: |
| Parameter AC-1(a): |
| Parameter AC-1(a)(1): |
| Parameter AC-1(b): |
| Parameter AC-1(c)(1)-1: |
| Parameter AC-1(c)(1)-2: |
| Parameter AC-1(c)(2)-1: |
| Parameter AC-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-1 What is the solution and how is it implemented?** |
|  |

**AC-2 Account Management**

1. Define and document the types of accounts allowed and specifically prohibited for use within the system;
2. Assign account managers;
3. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;
4. Specify:
   1. Authorized users of the system;
   2. Group and role membership; and
   3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;
5. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;
6. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];
7. Monitor the use of accounts;
8. Notify account managers and [Assignment: organization-defined personnel or roles] within:
   1. [Assignment: organization-defined time period] when accounts are no longer required;
   2. [Assignment: organization-defined time period] when users are terminated or transferred; and
   3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;
9. Authorize access to the system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. [Assignment: organization-defined attributes (as required)];
10. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];
11. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
12. Align account management processes with personnel termination and transfer processes.

|  |
| --- |
| **AC-2 Control Summary Information** |
| Responsible Role: |
| Parameter AC-2(c): |
| Parameter AC-2(d)(3): |
| Parameter AC-2(e): |
| Parameter AC-2(f): |
| Parameter AC-2(h): |
| Parameter AC-2(h)(1): |
| Parameter AC-2(h)(2): |
| Parameter AC-2(h)(3): |
| Parameter AC-2(i)(3): |
| Parameter AC-2(j): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-2 What is the solution and how is it implemented?** |
|  |

### 

**AC-2(1) Automated System Account Management**

Support the management of system accounts using [Assignment: organization-defined automated mechanisms].

|  |
| --- |
| **AC-2(1) Control Summary Information** |
| Responsible Role: |
| Parameter AC-2(1): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-2(1) What is the solution and how is it implemented?** |
|  |

### 

**AC-2(2) Automated Temporary and Emergency Account Management**

Automatically [Selection: remove; disable] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].

|  |
| --- |
| **AC-2(2) Control Summary Information** |
| Responsible Role: |
| Parameter AC-2(2)-1: |
| Parameter AC-2(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-2(2) What is the solution and how is it implemented?** |
|  |

### 

**AC-2(3) Disable Accounts**

Disable accounts within [Assignment: organization-defined time period] when the accounts:

(a) Have expired;

(b) Are no longer associated with a user or individual;

(c) Are in violation of organizational policy; or

(d) Have been inactive for [Assignment: organization-defined time period].

|  |
| --- |
| **AC-2(3) Control Summary Information** |
| Responsible Role: |
| Parameter AC-2(3): |
| Parameter AC-2(3)(d): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-2(3) What is the solution and how is it implemented?** |
|  |

### 

**AC-2(4) Automated Audit Actions**

Automatically audit account creation, modification, enabling, disabling, and removal actions.

|  |
| --- |
| **AC-2(4) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-2(4) What is the solution and how is it implemented?** |
|  |

### 

**AC-2(5) Inactivity Logout**

Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out].

|  |
| --- |
| **AC-2(5) Control Summary Information** |
| Responsible Role: |
| Parameter AC-2(5): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-2(5) What is the solution and how is it implemented?** |
|  |

### 

**AC-2(7) Privileged User Accounts**

(a) Establish and administer privileged user accounts in accordance with [Selection: Assignment: a role-based access scheme; an attribute-based access scheme];

(b) Monitor privileged role or attribute assignments;

(c) Monitor changes to roles or attributes; and

(d) Revoke access when privileged role or attribute assignments are no longer appropriate.

|  |
| --- |
| **AC-2(7) Control Summary Information** |
| Responsible Role: |
| Parameter AC-2(7)(a): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-2(7) What is the solution and how is it implemented?** |
|  |

### 

**AC-2(9) Restrictions on Use of Shared and Group Accounts**

Only permit the use of shared and group accounts that meet [Assignment: organization-defined conditions for establishing shared and group accounts].

|  |
| --- |
| **AC-2(9) Control Summary Information** |
| Responsible Role: |
| Parameter AC-2(9): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-2(9) What is the solution and how is it implemented?** |
|  |

### 

**AC-2(12) Account Monitoring for Atypical Usage**

(a) Monitor system accounts for [Assignment: organization-defined atypical usage]; and

(b) Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].

|  |
| --- |
| **AC-2(12) Control Summary Information** |
| Responsible Role: |
| Parameter AC-2(12)(a): |
| Parameter AC-2(12)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-2(12) What is the solution and how is it implemented?** |
|  |

**AC-2(13) Disable Accounts for High-risk Individuals**

Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].

|  |
| --- |
| **AC-2(13) Control Summary Information** |
| Responsible Role: |
| Parameter AC-2(13)-1: |
| Parameter AC-2(13)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-2(13) What is the solution and how is it implemented?** |
|  |

## 

**AC-3 Access Enforcement**

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

|  |
| --- |
| **AC-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-3 What is the solution and how is it implemented?** |
|  |

## 

**AC-4 Information Flow Enforcement**

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].

|  |
| --- |
| **AC-4 Control Summary Information** |
| Responsible Role: |
| Parameter AC-4: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-4 What is the solution and how is it implemented?** |
|  |

### 

**AC-4(21) Physical or Logical Separation of Information Flows**

Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].

|  |
| --- |
| **AC-4(21) Control Summary Information** |
| Responsible Role: |
| Parameter AC-4(21)-1: |
| Parameter AC-4(21)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-4(21) What is the solution and how is it implemented?** |
|  |

**AC-5 Separation of Duties**

a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and

b. Define system access authorizations to support separation of duties.

|  |
| --- |
| **AC-5 Control Summary Information** |
| Responsible Role: |
| Parameter AC-5(a): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-5 What is the solution and how is it implemented?** |
|  |

## 

**AC-6 Least Privilege**

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

|  |
| --- |
| **AC-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| AC-6 What is the solution and how is it implemented? |
|  |

### 

**AC-6(1) Authorize Access to Security Functions**

Authorize access for [Assignment: organization-defined individuals or roles] to:

(a) [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; and

(b) [Assignment: organization-defined security-relevant information].

|  |
| --- |
| **AC-6(1) Control Summary Information** |
| Responsible Role: |
| Parameter AC-6(1): |
| Parameter AC-6(1)(a): |
| Parameter AC-6(1)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-6(1) What is the solution and how is it implemented?** |
|  |

**AC-6(2) Non-privileged Access for Nonsecurity Functions**

Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing nonsecurity functions.

|  |
| --- |
| **AC-6(2) Control Summary Information** |
| Responsible Role: |
| Parameter AC-6(2): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-6(2) What is the solution and how is it implemented?** |
|  |

### 

**AC-6(5) Privileged Accounts**

Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].

|  |
| --- |
| **AC-6(5) Control Summary Information** |
| Responsible Role: |
| Parameter AC-6(5): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-6(5) What is the solution and how is it implemented?** |
|  |

### 

**AC-6(7) Review of User Privileges**

(a) Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and

(b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

|  |
| --- |
| **AC-6(7) Control Summary Information** |
| Responsible Role: |
| Parameter AC-6(7)(a)-1: |
| Parameter AC-6(7)(a)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-6(7) What is the solution and how is it implemented?** |
|  |

### 

**AC-6(9) Log Use of Privileged Functions**

Log the execution of privileged functions.

|  |
| --- |
| **AC-6(9) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-6(9) What is the solution and how is it implemented?** |
|  |

### 

**AC-6(10) Prohibit Non-privileged Users from Executing Privileged Functions**

Prevent non-privileged users from executing privileged functions.

|  |
| --- |
| **AC-6(10) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-6(10) What is the solution and how is it implemented?** |
|  |

## 

**AC-7 Unsuccessful Logon Attempts**

a. Enforce 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 (one-or-more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.

|  |
| --- |
| **AC-7 Control Summary Information** |
| Responsible Role: |
| Parameter AC-7(a)-1: |
| Parameter AC-7(a)-2: |
| Parameter AC-7(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-7 What is the solution and how is it implemented?** |
|  |

## 

**AC-8 System Use Notification**

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

1. Users are accessing a U.S. Government system;

2. System usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

4. Use of the system indicates consent to monitoring and recording;

b. Retain 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 system; and

c. For publicly accessible systems:

1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system

2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Include a description of the authorized uses of the system.

|  |
| --- |
| **AC-8 Control Summary Information** |
| Responsible Role: |
| Parameter AC-8(a): |
| Parameter AC-8(c)(1): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-8 What is the solution and how is it implemented?** |
|  |

## 

**AC-11 Device Lock**

a. Prevent further access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]; and

b. Retain the device lock until the user re-establishes access using established identification and authentication procedures.

|  |
| --- |
| **AC-11 Control Summary Information** |
| Responsible Role: |
| Parameter AC-11(a): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-11 What is the solution and how is it implemented?** |
|  |

### 

**AC-11(1) Pattern-hiding Displays**

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

|  |
| --- |
| **AC-11(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-11(1) What is the solution and how is it implemented?** |
|  |

## 

**AC-12 Session Termination**

Automatically terminate a user session after [Assignment: organization-defined conditions, or trigger events requiring session disconnect].

|  |
| --- |
| **AC-12 Control Summary Information** |
| Responsible Role: |
| Parameter AC-12: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-12 What is the solution and how is it implemented?** |
|  |

**AC-14 Permitted Actions Without Identification or Authentication**

a. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

|  |
| --- |
| **AC-14 Control Summary Information** |
| Responsible Role: |
| Parameter AC-14(a): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-14 What is the solution and how is it implemented?** |
|  |

## 

**AC-17 Remote Access**

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections.

|  |
| --- |
| **AC-17 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-17 What is the solution and how is it implemented?** |
|  |

### 

**AC-17(1) Monitoring and Control**

Employ automated mechanisms to monitor and control remote access methods.

|  |
| --- |
| **AC-17(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-17(1) What is the solution and how is it implemented?** |
|  |

**AC-17(2) Protection of Confidentiality and Integrity Using Encryption**

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

|  |
| --- |
| **AC-17(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-17(2) What is the solution and how is it implemented?** |
|  |

### 

**AC-17(3) Managed Access Control Points**

Route remote accesses through authorized and managed network access control points.

|  |
| --- |
| **AC-17(3) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-17(3) What is the solution and how is it implemented?** |
|  |

### 

**AC-17(4) Privileged Commands and Access**

(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs]; and

(b) Document the rationale for remote access in the security plan for the system.

|  |
| --- |
| **AC-17(4) Control Summary Information** |
| Responsible Role: |
| Parameter AC-17(4)(a): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-17(4) What is the solution and how is it implemented?** |
|  |

## 

**AC-18 Wireless Access**

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

b. Authorize each type of wireless access to the system prior to allowing such connections.

|  |
| --- |
| **AC-18 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-18 What is the solution and how is it implemented?** |
|  |

### 

**AC-18(1) Authentication and Encryption**

Protect wireless access to the system using authentication of [Selection (one-or-more): users; devices] and encryption.

|  |
| --- |
| **AC-18(1) Control Summary Information** |
| Responsible Role: |
| Parameter AC-18(1): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-18(1) What is the solution and how is it implemented?** |
|  |

### 

**AC-18(3) Disable Wireless Networking**

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

|  |
| --- |
| **AC-18(3) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-18(3) What is the solution and how is it implemented?** |
|  |

**AC-19 Access Control for Mobile Devices**

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems.

|  |
| --- |
| **AC-19 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-19 What is the solution and how is it implemented?** |
|  |

### 

**AC-19(5) Full Device or Container-based Encryption**

Employ [Selection: Assignment: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

|  |
| --- |
| **AC-19(5) Control Summary Information** |
| Responsible Role: |
| Parameter AC-19(5)-1: |
| Parameter AC-19(5)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-19(5) What is the solution and how is it implemented?** |
|  |

## 

**AC-20 Use of External Systems**

a. [Selection (one-or-more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

1. Access the system from external systems; and

2. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of [Assignment: organizationally-defined types of external systems].

|  |
| --- |
| **AC-20 Control Summary Information** |
| Responsible Role: |
| Parameter AC-20(a): |
| Parameter AC-20(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-20 What is the solution and how is it implemented?** |
|  |

### 

**AC-20(1) Limits on Authorized Use**

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

(a) Verification of the implementation of controls on the external system as specified in the organization’s security and privacy policies and security and privacy plans; or

(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

|  |
| --- |
| **AC-20(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-20(1) What is the solution and how is it implemented?** |
|  |

### 

**AC-20(2) Portable Storage Devices — Restricted Use**

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions].

|  |
| --- |
| **AC-20(2) Control Summary Information** |
| Responsible Role: |
| Parameter AC-20(2): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-20(2) What is the solution and how is it implemented?** |
|  |

## 

**AC-21 Information Sharing**

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information’s access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and

b. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions.

|  |
| --- |
| **AC-21 Control Summary Information** |
| Responsible Role: |
| Parameter AC-21(a): |
| Parameter AC-21(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-21 What is the solution and how is it implemented?** |
|  |

## 

**AC-22 Publicly Accessible Content**

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information [Assignment: organization-defined frequency] and remove such information, if discovered.

|  |
| --- |
| **AC-22 Control Summary Information** |
| Responsible Role: |
| Parameter AC-22(d): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AC-22 What is the solution and how is it implemented?** |
|  |

# 

**Awareness and Training**

**AT-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] awareness and training policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current awareness and training:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **AT-1 Control Summary Information** |
| Responsible Role: |
| Parameter AT-1(a): |
| Parameter AT-1(a)(1): |
| Parameter AT-1(b): |
| Parameter AT-1(c)(1)-1: |
| Parameter AT-1(c)(1)-2: |
| Parameter AT-1(c)(2)-1: |
| Parameter AT-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AT-1 What is the solution and how is it implemented?** |
|  |

## 

**AT-2 Literacy Training and Awareness**

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and

2. When required by system changes or following [Assignment: organization-defined events];

b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];

c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

d. Incorporate lessons learned from internal or external security or privacy incidents into literacy training and awareness techniques.

|  |
| --- |
| **AT-2 Control Summary Information** |
| Responsible Role: |
| Parameter AT-2(a)(1): |
| Parameter AT-2(a)(2): |
| Parameter AT-2(b): |
| Parameter AT-2(c)-1: |
| Parameter AT-2(c)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AT-2 What is the solution and how is it implemented?** |
|  |

### 

**AT-2(2) Insider Threat**

Provide literacy training on recognizing and reporting potential indicators of insider threat.

|  |
| --- |
| **AT-2(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AT-2(2) What is the solution and how is it implemented?** |
|  |

### 

**AT-2(3) Social Engineering and Mining**

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

|  |
| --- |
| **AT-2(3) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AT-2(3) What is the solution and how is it implemented?** |
|  |

## 

**AT-3 Role-based Training**

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:

1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and

2. When required by system changes;

b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

c. Incorporate lessons learned from internal or external security or privacy incidents into role-based training.

|  |
| --- |
| **AT-3 Control Summary Information** |
| Responsible Role: |
| Parameter AT-3(a): |
| Parameter AT-3(a)(1): |
| Parameter AT-3(b)-1: |
| Parameter AT-3(b)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AT-3 What is the solution and how is it implemented?** |
|  |

## 

**AT-4 Training Records**

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for [Assignment: organization-defined time period].

|  |
| --- |
| **AT-4 Control Summary Information** |
| Responsible Role: |
| Parameter AT-4(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AT-4 What is the solution and how is it implemented?** |
|  |

# 

**Audit and Accountability**

**AU-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] audit and accountability policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

c. Review and update the current audit and accountability:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **AU-1 Control Summary Information** |
| Responsible Role: |
| Parameter AU-1(a): |
| Parameter AU-1(a)(1): |
| Parameter AU-1(b): |
| Parameter AU-1(c)(1)-1: |
| Parameter AU-1(c)(1)-2: |
| Parameter AU-1(c)(2)-1: |
| Parameter AU-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-1 What is the solution and how is it implemented?** |
|  |

## 

**AU-2 Event Logging**

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: [[Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

|  |
| --- |
| **AU-2 Control Summary Information** |
| Responsible Role: |
| Parameter AU-2(a): |
| Parameter AU-2(c): |
| Parameter AU-2(e): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-2 What is the solution and how is it implemented?** |
|  |

## 

**AU-3 Content of Audit Records**

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

|  |
| --- |
| **AU-3 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-3 What is the solution and how is it implemented?** |
|  |

### 

**AU-3(1) Additional Audit Information**

Generate audit records containing the following additional information: [Assignment: organization-defined additional information].

|  |
| --- |
| **AU-3(1) Control Summary Information** |
| Responsible Role: |
| Parameter AU-3(1): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-3(1) What is the solution and how is it implemented?** |
|  |

## 

**AU-4 Audit Log Storage Capacity**

Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].

|  |
| --- |
| **AU-4 Control Summary Information** |
| Responsible Role: |
| Parameter AU-4: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-4 What is the solution and how is it implemented?** |
|  |

## 

**AU-5 Response to Audit Logging Process Failures**

a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; and

b. Take the following additional actions: [Assignment: organization-defined additional actions].

|  |
| --- |
| **AU-5 Control Summary Information** |
| Responsible Role: |
| Parameter AU-5(a)-1: |
| Parameter AU-5(a)-2: |
| Parameter AU-5(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-5 What is the solution and how is it implemented?** |
|  |

## 

**AU-6 Audit Record Review, Analysis, and Reporting**

a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;

b. Report findings to [Assignment: organization-defined personnel or roles]; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

|  |
| --- |
| **AU-6 Control Summary Information** |
| Responsible Role: |
| Parameter AU-6(a)-1: |
| Parameter AU-6(a)-2: |
| Parameter AU-6(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-6 What is the solution and how is it implemented?** |
|  |

### 

**AU-6(1) Automated Process Integration**

Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].

|  |
| --- |
| **AU-6(1) Control Summary Information** |
| Responsible Role: |
| Parameter AU-6(1): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-6(1) What is the solution and how is it implemented?** |
|  |

**AU-6(3) Correlate Audit Record Repositories**

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

|  |
| --- |
| **AU-6(3) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-6(3) What is the solution and how is it implemented?** |
|  |

## 

**AU-7 Audit Record Reduction and Report Generation**

Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and

b. Does not alter the original content or time ordering of audit records.

|  |
| --- |
| **AU-7 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-7 What is the solution and how is it implemented?** |
|  |

### 

**AU-7(1) Automatic Processing**

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records].

|  |
| --- |
| **AU-7(1) Control Summary Information** |
| Responsible Role: |
| Parameter AU-7(1): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-7(1) What is the solution and how is it implemented?** |
|  |

## 

**AU-8 Time Stamps**

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

|  |
| --- |
| **AU-8 Control Summary Information** |
| Responsible Role: |
| Parameter AU-8(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-8 What is the solution and how is it implemented?** |
|  |

## 

**AU-9 Protection of Audit Information**

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.

|  |
| --- |
| **AU-9 Control Summary Information** |
| Responsible Role: |
| Parameter AU-9(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-9 What is the solution and how is it implemented?** |
|  |

### 

**AU-9(4) Access by Subset of Privileged Users**

Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].

|  |
| --- |
| **AU-9(4) Control Summary Information** |
| Responsible Role: |
| Parameter AU-9(4): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-9(4) What is the solution and how is it implemented?** |
|  |

## 

**AU-11 Audit Record Retention**

Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

|  |
| --- |
| **AU-11 Control Summary Information** |
| Responsible Role: |
| Parameter AU-11: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-11 What is the solution and how is it implemented?** |
|  |

## 

**AU-12 Audit Record Generation**

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components];

b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

|  |
| --- |
| **AU-12 Control Summary Information** |
| Responsible Role: |
| Parameter AU-12(a): |
| Parameter AU-12(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **AU-12 What is the solution and how is it implemented?** |
|  |

# 

**Assessment, Authorization, and Monitoring**

**CA-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] assessment, authorization, and monitoring policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **CA-1 Control Summary Information** |
| Responsible Role: |
| Parameter CA-1(a): |
| Parameter CA-1(a)(1): |
| Parameter CA-1(b): |
| Parameter CA-1(c)(1)-1: |
| Parameter CA-1(c)(1)-2: |
| Parameter CA-1(c)(2)-1: |
| Parameter CA-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-1 What is the solution and how is it implemented?** |
|  |

**CA-2 Control Assessments**

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. Develop a control assessment plan that describes the scope of the assessment including:

1. Controls and control enhancements under assessment;

2. Assessment procedures to be used to determine control effectiveness; and

3. Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

d. Assess the controls in the 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 and privacy

e. Produce a control assessment report that document the results of the assessment; and

f. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].

|  |
| --- |
| **CA-2 Control Summary Information** |
| Responsible Role: |
| Parameter CA-2(d): |
| Parameter CA-2(f): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-2 What is the solution and how is it implemented?** |
|  |

### 

**CA-2(1) Independent Assessors**

Employ independent assessors or assessment teams to conduct control assessments.

|  |
| --- |
| **CA-2(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-2(1) What is the solution and how is it implemented?** |
|  |

### 

**CA-2(3) Leveraging Results from External Organizations**

Leverage the results of control assessments performed by [Assignment: organization-defined external organization] on [Assignment: organization-defined system] when the assessment meets [Assignment: organization-defined requirements].

|  |
| --- |
| **CA-2(3) Control Summary Information** |
| Responsible Role: |
| Parameter CA-2(3)-1: |
| Parameter CA-2(3)-2: |
| Parameter CA-2(3)-3: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-2(3) What is the solution and how is it implemented?** |
|  |

## 

**CA-3 Information Exchange**

a. Approve and manage the exchange of information between the system and other systems using [Selection (one-or-more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements, [Assignment: organization-defined type of agreement]];

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the agreements [Assignment: organization-defined frequency].

|  |
| --- |
| **CA-3 Control Summary Information** |
| Responsible Role: |
| Parameter CA-3(a): |
| Parameter CA-3(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-3 What is the solution and how is it implemented?** |
|  |

## 

**CA-5 Plan of Action and Milestones**

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

|  |
| --- |
| **CA-5 Control Summary Information** |
| Responsible Role: |
| Parameter CA-5(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-5 What is the solution and how is it implemented?** |
|  |

## 

**CA-6 Authorization**

a. Assign a senior official as the authorizing official for the system;

b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:

1. Accepts the use of common controls inherited by the system; and

2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;

e. Update the authorizations [Assignment: organization-defined frequency].

|  |
| --- |
| **CA-6 Control Summary Information** |
| Responsible Role: |
| Parameter CA-6(e): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-6 What is the solution and how is it implemented?** |
|  |

## 

**CA-7 Continuous Monitoring**

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];

b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

|  |
| --- |
| **CA-7 Control Summary Information** |
| Responsible Role: |
| Parameter CA-7(a): |
| Parameter CA-7(b)-1: |
| Parameter CA-7(b)-2: |
| Parameter CA-7(g)-1: |
| Parameter CA-7(g)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-7 What is the solution and how is it implemented?** |
|  |

### 

**CA-7(1) Independent Assessment**

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

|  |
| --- |
| **CA-7(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-7(1) What is the solution and how is it implemented?** |
|  |

### 

**CA-7(4) Risk Monitoring**

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

(a) Effectiveness monitoring;

(b) Compliance monitoring; and

(c) Change monitoring.

|  |
| --- |
| **CA-7(4) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-7(4) What is the solution and how is it implemented?** |
|  |

## 

**CA-8 Penetration Testing**

Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].

|  |
| --- |
| **CA-8 Control Summary Information** |
| Responsible Role: |
| Parameter CA-8-1: |
| Parameter CA-8-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-8 What is the solution and how is it implemented?** |
|  |

### 

**CA-8(1) Independent Penetration Testing Agent or Team**

Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

|  |
| --- |
| **CA-8(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-8(1) What is the solution and how is it implemented?** |
|  |

### 

**CA-8(2) Red Team Exercises**

Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises].

|  |
| --- |
| **CA-8(2) Control Summary Information** |
| Responsible Role: |
| Parameter CA-8(2): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-8(2) What is the solution and how is it implemented?** |
|  |

## 

**CA-9 Internal System Connections**

a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system;

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

c. Terminate internal system connections after [Assignment: organization-defined conditions]; and

d. Review [Assignment: organization-defined frequency] the continued need for each internal connection.

|  |
| --- |
| **CA-9 Control Summary Information** |
| Responsible Role: |
| Parameter CA-9(a): |
| Parameter CA-9(c): |
| Parameter CA-9(d): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CA-9 What is the solution and how is it implemented?** |
|  |

# 

**Configuration Management**

**CM-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] configuration management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and

c. Review and update the current configuration management:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **CM-1 Control Summary Information** |
| Responsible Role: |
| Parameter CM-1(a): |
| Parameter CM-1(a)(1): |
| Parameter CM-1(b): |
| Parameter CM-1(c)(1)-1: |
| Parameter CM-1(c)(1)-2: |
| Parameter CM-1(c)(2)-1: |
| Parameter CM-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-1 What is the solution and how is it implemented?** |
|  |

## 

**CM-2 Baseline Configuration**

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:

1. [Assignment: organization-defined frequency];

2. When required due to [Assignment: organization-defined circumstances]; and

3. When system components are installed or upgraded.

|  |
| --- |
| **CM-2 Control Summary Information** |
| Responsible Role: |
| Parameter CM-2(b)(1): |
| Parameter CM-2(b)(2): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-2 What is the solution and how is it implemented?** |
|  |

### 

**CM-2(2) Automation Support for Accuracy and Currency**

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].

|  |
| --- |
| **CM-2(2) Control Summary Information** |
| Responsible Role: |
| Parameter CM-2(2): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-2(2) What is the solution and how is it implemented?** |
|  |

**CM-2(3) Retention of Previous Configurations**

Retain [Assignment: organization-defined number] of previous versions of baseline configurations of the system to support rollback.

|  |
| --- |
| **CM-2(3) Control Summary Information** |
| Responsible Role: |
| Parameter CM-2(3): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-2(3) What is the solution and how is it implemented?** |
|  |

### 

**CM-2(7) Configure Systems and Components for High-risk Areas**

(a) Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and

(b) Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls].

|  |
| --- |
| **CM-2(7) Control Summary Information** |
| Responsible Role: |
| Parameter CM-2(7)(a)-1: |
| Parameter CM-2(7)(a)-2: |
| Parameter CM-2(7)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-2(7) What is the solution and how is it implemented?** |
|  |

## 

**CM-3 Configuration Change Control**

a. Determine and document the types of changes to the system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

c. Document configuration change decisions associated with the system;

d. Implement approved configuration-controlled changes to the system;

e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];

f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one-or-more): organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].

|  |
| --- |
| **CM-3 Control Summary Information** |
| Responsible Role: |
| Parameter CM-3(e): |
| Parameter CM-3(g)-1: |
| Parameter CM-3(g)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-3 What is the solution and how is it implemented?** |
|  |

### 

**CM-3(2) Testing, Validation, and Documentation of Changes**

Test, validate, and document changes to the system before finalizing the implementation of the changes.

|  |
| --- |
| **CM-3(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-3(2) What is the solution and how is it implemented?** |
|  |

### 

**CM-3(4) Security and Privacy Representatives**

Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].

|  |
| --- |
| **CM-3(4) Control Summary Information** |
| Responsible Role: |
| Parameter CM-3(4)-1: |
| Parameter CM-3(4)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-3(4) What is the solution and how is it implemented?** |
|  |

## 

**CM-4 Impact Analyses**

Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

|  |
| --- |
| **CM-4 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-4 What is the solution and how is it implemented?** |
|  |

### 

**CM-4(2) Verification of Controls**

After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

|  |
| --- |
| **CM-4(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-4(2) What is the solution and how is it implemented?** |
|  |

**CM-5 Access Restrictions for Change**

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

|  |
| --- |
| **CM-5 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-5 What is the solution and how is it implemented?** |
|  |

### 

**CM-5(1) Automated Access Enforcement and Audit Records**

(a) Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and

(b) Automatically generate audit records of the enforcement actions.

|  |
| --- |
| **CM-5(1) Control Summary Information** |
| Responsible Role: |
| Parameter CM-5(1)(a): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-5(1) What is the solution and how is it implemented?** |
|  |

### 

**CM-5(5) Privilege Limitation for Production and Operation**

(a) Limit privileges to change system components and system-related information within a production or operational environment; and

(b) Review and reevaluate privileges [Assignment: organization-defined frequency].

|  |
| --- |
| **CM-5(5) Control Summary Information** |
| Responsible Role: |
| Parameter CM-5(5)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-5(5) What is the solution and how is it implemented?** |
|  |

## 

**CM-6 Configuration Settings**

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

|  |
| --- |
| **CM-6 Control Summary Information** |
| Responsible Role: |
| Parameter CM-6(a): |
| Parameter CM-6(c)-1: |
| Parameter CM-6(c)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-6 What is the solution and how is it implemented?** |
|  |

### 

**CM-6(1) Automated Management, Application, and Verification**

Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].

|  |
| --- |
| **CM-6(1) Control Summary Information** |
| Responsible Role: |
| Parameter CM-6(1)-1: |
| Parameter CM-6(1)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-6(1) What is the solution and how is it implemented?** |
|  |

## 

**CM-7 Least Functionality**

a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].

|  |
| --- |
| **CM-7 Control Summary Information** |
| Responsible Role: |
| Parameter CM-7(a): |
| Parameter CM-7(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-7 What is the solution and how is it implemented?** |
|  |

### 

**CM-7(1) Periodic Review**

(a) Review the system [Assignment: organization-defined mission essential capabilities] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

(b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].

|  |
| --- |
| **CM-7(1) Control Summary Information** |
| Responsible Role: |
| Parameter CM-7(1)(a): |
| Parameter CM-7(1)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-7(1) What is the solution and how is it implemented?** |
|  |

**CM-7(2) Prevent Program Execution**

Prevent program execution in accordance with [Selection (one-or-more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].

|  |
| --- |
| **CM-7(2) Control Summary Information** |
| Responsible Role: |
| Parameter CM-7(2): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-7(2) What is the solution and how is it implemented?** |
|  |

**CM-7(5) Authorized Software**

(a) Identify [Assignment: organization-defined software programs authorized to execute on the system];

(b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and

(c) Review and update the list of authorized software programs [Assignment: organization-defined frequency].

|  |
| --- |
| **CM-7(5) Control Summary Information** |
| Responsible Role: |
| Parameter CM-7(5)(a): |
| Parameter CM-7(5)(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-7(5) What is the solution and how is it implemented?** |
|  |

**CM-8 System Component Inventory**

a. Develop and document an inventory of system components that:

1. Accurately reflects the system;

2. Includes all components within the system;

3. Does not include duplicate accounting of components or components assigned to any other system;

4. Is at the level of granularity deemed necessary for tracking and reporting; and

5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and

b. Review and update the system component inventory [Assignment: organization-defined frequency].

|  |
| --- |
| **CM-8 Control Summary Information** |
| Responsible Role: |
| Parameter CM-8(a)(5): |
| Parameter CM-8(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-8 What is the solution and how is it implemented?** |
|  |

**CM-8(1) Updates During Installation and Removal**

Update the inventory of system components as part of component installations, removals, and system updates.

|  |
| --- |
| **CM-8(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-8(1) What is the solution and how is it implemented?** |
|  |

**CM-8(3) Automated Unauthorized Component Detection**

(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency; and

(b) Take the following actions when unauthorized components are detected: [Selection (one-or-more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].

|  |
| --- |
| **CM-8(3) Control Summary Information** |
| Responsible Role: |
| Parameter CM-8(3)(a)-1: |
| Parameter CM-8(3)(a)-2: |
| Parameter CM-8(3)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-8(3) What is the solution and how is it implemented?** |
|  |

**CM-9 Configuration Management Plan**

Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the system and places the configuration items under configuration management;

d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; and

e. Protects the configuration management plan from unauthorized disclosure and modification.

|  |
| --- |
| **CM-9 Control Summary Information** |
| Responsible Role: |
| Parameter CM-9(d): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-9 What is the solution and how is it implemented?** |
|  |

**CM-10 Software Usage Restrictions**

a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

|  |
| --- |
| **CM-10 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-10 What is the solution and how is it implemented?** |
|  |

**CM-11 User-installed Software**

a. Establish [Assignment: organization-defined policies] governing the installation of software by users;

b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and

c. Monitor policy compliance [Assignment: organization-defined frequency].

|  |
| --- |
| **CM-11 Control Summary Information** |
| Responsible Role: |
| Parameter CM-11(a): |
| Parameter CM-11(b): |
| Parameter CM-11(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-11 What is the solution and how is it implemented?** |
|  |

**CM-12 Information Location**

a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

|  |
| --- |
| **CM-12 Control Summary Information** |
| Responsible Role: |
| Parameter CM-12(a): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-12 What is the solution and how is it implemented?** |
|  |

**CM-12(1) Automated Tools to Support Information Location**

Use automated tools to identify [Assignment: organization-defined information by information type] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy.

|  |
| --- |
| **CM-12(1) Control Summary Information** |
| Responsible Role: |
| Parameter CM-12(1)-1: |
| Parameter CM-12(1)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CM-12(1) What is the solution and how is it implemented?** |
|  |

**Contingency Planning**

**CP-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] contingency planning policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **CP-1 Control Summary Information** |
| Responsible Role: |
| Parameter CP-1(a): |
| Parameter CP-1(a)(1): |
| Parameter CP-1(b): |
| Parameter CP-1(c)(1)-1: |
| Parameter CP-1(c)(1)-2: |
| Parameter CP-1(c)(2)-1: |
| Parameter CP-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-1 What is the solution and how is it implemented?** |
|  |

**CP-2 Contingency Plan**

a. Develop a contingency plan for the system that:

1. Identifies essential mission and business functions and associated contingency requirements;

2. Provides recovery objectives, restoration priorities, and metrics;

3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;

5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;

6. Addresses the sharing of contingency information; and

7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];

b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system [Assignment: organization-defined frequency];

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect the contingency plan from unauthorized disclosure and modification.

|  |
| --- |
| **CP-2 Control Summary Information** |
| Responsible Role: |
| Parameter CP-2(a)(7): |
| Parameter CP-2(b): |
| Parameter CP-2(d): |
| Parameter CP-2(f): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-2 What is the solution and how is it implemented?** |
|  |

**CP-2(1) Coordinate with Related Plans**

Coordinate contingency plan development with organizational elements responsible for related plans.

|  |
| --- |
| **CP-2(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-2(1) What is the solution and how is it implemented?** |
|  |

**CP-2(3) Resume Mission and Business Functions**

Plan for the resumption of [Selection: all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.

|  |
| --- |
| **CP-2(3) Control Summary Information** |
| Responsible Role: |
| Parameter CP-2(3)-1: |
| Parameter CP-2(3)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-2(3) What is the solution and how is it implemented?** |
|  |

**CP-2(8) Identify Critical Assets**

Identify critical system assets supporting [Selection: Assignment: all; essential] mission and business functions.

|  |
| --- |
| **CP-2(8) Control Summary Information** |
| Responsible Role: |
| Parameter CP-2(8): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-2(8) What is the solution and how is it implemented?** |
|  |

**CP-3 Contingency Training**

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

1. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;

2. When required by system changes; and

3. [Assignment: organization-defined frequency] thereafter; and

b. Review and update contingency training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **CP-3 Control Summary Information** |
| Responsible Role: |
| Parameter CP-3(a)(1): |
| Parameter CP-3(a)(3): |
| Parameter CP-3(b)-1: |
| Parameter CP-3(b)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-3 What is the solution and how is it implemented?** |
|  |

**CP-4 Contingency Plan Testing**

a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

|  |
| --- |
| **CP-4 Control Summary Information** |
| Responsible Role: |
| Parameter CP-4(a)-1: |
| Parameter CP-4(a)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-4 What is the solution and how is it implemented?** |
|  |

**CP-4(1) Coordinate with Related Plans**

Coordinate contingency plan testing with organizational elements responsible for related plans.

|  |
| --- |
| **CP-4(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-4(1) What is the solution and how is it implemented?** |
|  |

**CP-6 Alternate Storage Site**

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

|  |
| --- |
| **CP-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-6 What is the solution and how is it implemented?** |
|  |

**CP-6(1) Separation from Primary Site**

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

|  |
| --- |
| **CP-6(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-6(1) What is the solution and how is it implemented?** |
|  |

**CP-6(3) Accessibility**

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

|  |
| --- |
| **CP-6(3) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-6(3) What is the solution and how is it implemented?** |
|  |

**CP-7 Alternate Processing Site**

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

|  |
| --- |
| **CP-7 Control Summary Information** |
| Responsible Role: |
| Parameter CP-7(a)-1: |
| Parameter CP-7(a)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-7 What is the solution and how is it implemented?** |
|  |

**CP-7(1) Separation from Primary Site**

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

|  |
| --- |
| **CP-7(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-7(1) What is the solution and how is it implemented?** |
|  |

**CP-7(2) Accessibility**

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

|  |
| --- |
| **CP-7(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-7(2) What is the solution and how is it implemented?** |
|  |

**CP-7(3) Priority of Service**

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

|  |
| --- |
| **CP-7(3) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-7(3) What is the solution and how is it implemented?** |
|  |

**CP-8 Telecommunications Services**

Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

|  |
| --- |
| **CP-8 Control Summary Information** |
| Responsible Role: |
| Parameter CP-8-1: |
| Parameter CP-8-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-8 What is the solution and how is it implemented?** |
|  |

**CP-8(1) Priority of Service Provisions**

(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and

(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

|  |
| --- |
| **CP-8(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-8(1) What is the solution and how is it implemented?** |
|  |

**CP-8(2) Single Points of Failure**

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

|  |
| --- |
| **CP-8(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-8(2) What is the solution and how is it implemented?** |
|  |

**CP-9 System Backup**

a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];

b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];

c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and

d. Protect the confidentiality, integrity, and availability of backup information.

|  |
| --- |
| **CP-9 Control Summary Information** |
| Responsible Role: |
| Parameter CP-9(a)-1: |
| Parameter CP-9(a)-2: |
| Parameter CP-9(b): |
| Parameter CP-9(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-9 What is the solution and how is it implemented?** |
|  |

**CP-9(1) Testing for Reliability and Integrity**

Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.

|  |
| --- |
| **CP-9(1) Control Summary Information** |
| Responsible Role: |
| Parameter CP-9(1): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-9(1) What is the solution and how is it implemented?** |
|  |

**CP-9(8) Cryptographic Protection**

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].

|  |
| --- |
| **CP-9(8) Control Summary Information** |
| Responsible Role: |
| Parameter CP-9(8): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-9(8) What is the solution and how is it implemented?** |
|  |

**CP-10 System Recovery and Reconstitution**

Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.

|  |
| --- |
| **CP-10 Control Summary Information** |
| Responsible Role: |
| Parameter CP-10: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-10 What is the solution and how is it implemented?** |
|  |

**CP-10(2) Transaction Recovery**

Implement transaction recovery for systems that are transaction-based.

|  |
| --- |
| **CP-10(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **CP-10(2) What is the solution and how is it implemented?** |
|  |

**Identification and Authentication**

**IA-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] identification and authentication policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **IA-1 Control Summary Information** |
| Responsible Role: |
| Parameter IA-1(a): |
| Parameter IA-1(a)(1): |
| Parameter IA-1(b): |
| Parameter IA-1(c)(1)-1: |
| Parameter IA-1(c)(1)-2: |
| Parameter IA-1(c)(2)-1: |
| Parameter IA-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-1 What is the solution and how is it implemented?** |
|  |

**IA-2 Identification and Authentication (Organizational Users)**

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

|  |
| --- |
| **IA-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-2 What is the solution and how is it implemented?** |
|  |

**IA-2(1) Multi-factor Authentication to Privileged Accounts**

Implement multi-factor authentication for access to privileged accounts.

|  |
| --- |
| **IA-2(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-2(1) What is the solution and how is it implemented?** |
|  |

**IA-2(2) Multi-factor Authentication to Non-privileged Accounts**

Implement multi-factor authentication for access to non-privileged accounts.

|  |
| --- |
| **IA-2(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-2(2) What is the solution and how is it implemented?** |
|  |

**IA-2(5) Individual Authentication with Group Authentication**

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

|  |
| --- |
| **IA-2(5) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-2(5) What is the solution and how is it implemented?** |
|  |

**IA-2(6) Access to Accounts —separate Device**

Implement multi-factor authentication for [Selection (one or more): local; network; remote] access to [Selection (one or more): privileged accounts; non-privileged accounts] such that:

(a) One of the factors is provided by a device separate from the system gaining access; and

(b) The device meets [Assignment: organization-defined strength of mechanism requirements].

|  |
| --- |
| **IA-2(6) Control Summary Information** |
| Responsible Role: |
| Parameter IA-2(6)-1: |
| Parameter IA-2(6)-2: |
| Parameter IA-2(6)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-2(6) What is the solution and how is it implemented?** |
|  |

**IA-2(8) Access to Accounts — Replay Resistant**

Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].

|  |
| --- |
| **IA-2(8) Control Summary Information** |
| Responsible Role: |
| Parameter IA-2(8): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-2(8) What is the solution and how is it implemented?** |
|  |

**IA-2(12) Acceptance of PIV Credentials**

Accept and electronically verify Personal Identity Verification-compliant credentials.

|  |
| --- |
| **IA-2(12) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-2(12) What is the solution and how is it implemented?** |
|  |

**IA-3 Device Identification and Authentication**

Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one-or-more): local; remote; network] connection.

|  |
| --- |
| **IA-3 Control Summary Information** |
| Responsible Role: |
| Parameter IA-3-1: |
| Parameter IA-3-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-3 What is the solution and how is it implemented?** |
|  |

**IA-4 Identifier Management**

Manage system identifiers by:

a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers for [Assignment: organization-defined time period].

|  |
| --- |
| **IA-4 Control Summary Information** |
| Responsible Role: |
| Parameter IA-4(a): |
| Parameter IA-4(d): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-4 What is the solution and how is it implemented?** |
|  |

**IA-4(4) Identify User Status**

Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].

|  |
| --- |
| **IA-4(4) Control Summary Information** |
| Responsible Role: |
| Parameter IA-4(4): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-4(4) What is the solution and how is it implemented?** |
|  |

**IA-5 Authenticator Management**

Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued 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 or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

|  |
| --- |
| **IA-5 Control Summary Information** |
| Responsible Role: |
| Parameter IA-5(f)-1: |
| Parameter IA-5(f)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-5 What is the solution and how is it implemented?** |
|  |

**IA-5(1) Password-based Authentication**

For password-based authentication:

(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;

(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);

(c) Transmit passwords only over cryptographically-protected channels;

(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;

(e) Require immediate selection of a new password upon account recovery;

(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;

(g) Employ automated tools to assist the user in selecting strong password authenticators; and

(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

|  |
| --- |
| **IA-5(1) Control Summary Information** |
| Responsible Role: |
| Parameter IA-5(1)(a): |
| Parameter IA-5(1)(h): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-5(1) What is the solution and how is it implemented?** |
|  |

**IA-5(2) Public Key-based Authentication**

1. For public key-based authentication:
2. Enforce authorized access to the corresponding private key; and
3. Map the authenticated identity to the account of the individual or group; and

(b) When public key infrastructure (PKI) is used:

(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and

(2) Implement a local cache of revocation data to support path discovery and validation.

|  |
| --- |
| **IA-5(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-5(2) What is the solution and how is it implemented?** |
|  |

**IA-5(6) Protection of Authenticators**

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

|  |
| --- |
| **IA-5(6) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-5(6) What is the solution and how is it implemented?** |
|  |

**IA-5(7) No Embedded Unencrypted Static Authenticators**

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

|  |
| --- |
| **IA-5(7) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-5(7) What is the solution and how is it implemented?** |
|  |

**IA-6 Authentication Feedback**

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

|  |
| --- |
| **IA-6 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-6 What is the solution and how is it implemented?** |
|  |

**IA-7 Cryptographic Module Authentication**

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

|  |
| --- |
| **IA-7 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-7 What is the solution and how is it implemented?** |
|  |

**IA-8 Identification and Authentication (Non-organizational Users)**

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

|  |
| --- |
| **IA-8 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-8 What is the solution and how is it implemented?** |
|  |

**IA-8(1) Acceptance of PIV Credentials from Other Agencies**

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

|  |
| --- |
| **IA-8(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-8(1) What is the solution and how is it implemented?** |
|  |

**IA-8(2) Acceptance of External Authenticators**

(a) Accept only external authenticators that are NIST-compliant; and

(b) Document and maintain a list of accepted external authenticators.

|  |
| --- |
| **IA-8(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-8(2) What is the solution and how is it implemented?** |
|  |

**IA-8(4) Use of Defined Profiles**

Conform to the following profiles for identity management [Assignment: organization-defined identity management profiles].

|  |
| --- |
| **IA-8(4) Control Summary Information** |
| Responsible Role: |
| Parameter IA-8(4): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-8(4) What is the solution and how is it implemented?** |
|  |

**IA-11 Re-authentication**

Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].

|  |
| --- |
| **IA-11 Control Summary Information** |
| Responsible Role: |
| Parameter IA-11: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-11 What is the solution and how is it implemented?** |
|  |

**IA-12 Identity Proofing**

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

|  |
| --- |
| **IA-12 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-12 What is the solution and how is it implemented?** |
|  |

**IA-12(2) Identity Evidence**

Require evidence of individual identification be presented to the registration authority.

|  |
| --- |
| **IA-12(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-12(2) What is the solution and how is it implemented?** |
|  |

**IA-12(3) Identity Evidence Validation and Verification**

Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].

|  |
| --- |
| **IA-12(3) Control Summary Information** |
| Responsible Role: |
| Parameter IA-12(3): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-12(3) What is the solution and how is it implemented?** |
|  |

**IA-12(5) Address Confirmation**

Require that a [Selection: Assignment: registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

|  |
| --- |
| **IA-12(5) Control Summary Information** |
| Responsible Role: |
| Parameter IA-12(5): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IA-12(5) What is the solution and how is it implemented?** |
|  |

**Incident Response**

**IR-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] incident response policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **IR-1 Control Summary Information** |
| Responsible Role: |
| Parameter IR-1(a): |
| Parameter IR-1(a)(1): |
| Parameter IR-1(b): |
| Parameter IR-1(c)(1)-1: |
| Parameter IR-1(c)(1)-2: |
| Parameter IR-1(c)(2)-1: |
| Parameter IR-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-1 What is the solution and how is it implemented?** |
|  |

**IR-2 Incident Response Training**

a. Provide incident response training to system users consistent with assigned roles and responsibilities:

1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access;

2. When required by system changes; and

3. [Assignment: organization-defined frequency] thereafter; and

b. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **IR-2 Control Summary Information** |
| Responsible Role: |
| Parameter IR-2(a)(1): |
| Parameter IR-2(a)(3): |
| Parameter IR-2(b)-1: |
| Parameter IR-2(b)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-2 What is the solution and how is it implemented?** |
|  |

**IR-3 Incident Response Testing**

Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].

|  |
| --- |
| **IR-3 Control Summary Information** |
| Responsible Role: |
| Parameter IR-3-1: |
| Parameter IR-3-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-3 What is the solution and how is it implemented?** |
|  |

**IR-3(2) Coordination with Related Plans**

Coordinate incident response testing with organizational elements responsible for related plans.

|  |
| --- |
| **IR-3(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-3(2) What is the solution and how is it implemented?** |
|  |

**IR-4 Incident Handling**

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinate incident handling activities with contingency planning activities;

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

|  |
| --- |
| **IR-4 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-4 What is the solution and how is it implemented?** |
|  |

**IR-4(1) Automated Incident Handling Processes**

Support the incident handling process using [Assignment: organization-defined automated mechanisms].

|  |
| --- |
| **IR-4(1) Control Summary Information** |
| Responsible Role: |
| Parameter IR-4(1): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-4(1) What is the solution and how is it implemented?** |
|  |

**IR-5 Incident Monitoring**

Track and document incidents.

|  |
| --- |
| **IR-5 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-5 What is the solution and how is it implemented?** |
|  |

**IR-6 Incident Reporting**

a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and

b. Report incident information to [Assignment: organization-defined authorities].

|  |
| --- |
| **IR-6 Control Summary Information** |
| Responsible Role: |
| Parameter IR-6(a): |
| Parameter IR-6(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-6 What is the solution and how is it implemented?** |
|  |

**IR-6(1) Automated Reporting**

Report incidents using [Assignment: organization-defined automated mechanisms].

|  |
| --- |
| **IR-6(1) Control Summary Information** |
| Responsible Role: |
| Parameter IR-6(1): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-6(1) What is the solution and how is it implemented?** |
|  |

**IR-6(3) Supply Chain Coordination**

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

|  |
| --- |
| **IR-6(3) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-6(3) What is the solution and how is it implemented?** |
|  |

**IR-7 Incident Response Assistance**

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

|  |
| --- |
| **IR-7 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-7 What is the solution and how is it implemented?** |
|  |

**IR-7(1) Automation Support for Availability of Information and Support**

Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms].

|  |
| --- |
| **IR-7(1) Control Summary Information** |
| Responsible Role: |
| Parameter IR-7(1): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-7(1) What is the solution and how is it implemented?** |
|  |

**IR-8 Incident Response Plan**

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;

2. Describes the structure and organization of the incident response capability;

3. Provides a high-level approach for how the incident response capability fits into the overall organization;

4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

5. Defines reportable incidents;

6. Provides metrics for measuring the incident response capability within the organization;

7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;

8. Addresses the sharing of incident information;

9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and

10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles].

b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and

e. Protect the incident response plan from unauthorized disclosure and modification.

|  |
| --- |
| **IR-8 Control Summary Information** |
| Responsible Role: |
| Parameter IR-8(a)(9)-1: |
| Parameter IR-8(a)(9)-2: |
| Parameter IR-8(a)(10): |
| Parameter IR-8(b): |
| Parameter IR-8(d): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-8 What is the solution and how is it implemented?** |
|  |

**IR-9 Information Spillage Response**

Respond to information spills by:

a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;

b. Identifying the specific information involved in the system contamination;

c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;

d. Isolating the contaminated system or system component;

e. Eradicating the information from the contaminated system or component;

f. Identifying other systems or system components that may have been subsequently contaminated; and

g. Performing the following additional actions: [Assignment: organization-defined actions].

|  |
| --- |
| **IR-9 Control Summary Information** |
| Responsible Role: |
| Parameter IR-9(a): |
| Parameter IR-9(c): |
| Parameter IR-9(g): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-9 What is the solution and how is it implemented?** |
|  |

**IR-9(2) Training**

Provide information spillage response training [Assignment: organization-defined frequency].

|  |
| --- |
| **IR-9(2) Control Summary Information** |
| Responsible Role: |
| Parameter IR-9(2): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-9(2) What is the solution and how is it implemented?** |
|  |

**IR-9(3) Post-spill Operations**

Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective [Assignment: organization-defined procedures]

|  |
| --- |
| **IR-9(3) Control Summary Information** |
| Responsible Role: |
| Parameter IR-9(3): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-9(3) What is the solution and how is it implemented?** |
|  |

**IR-9(4) Exposure to Unauthorized Personnel**

Employ the following controls for personnel exposed to information not within assigned access authorizations: [Assignment: organization-defined controls].

|  |
| --- |
| **IR-9(4) Control Summary Information** |
| Responsible Role: |
| Parameter IR-9(4): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **IR-9(4) What is the solution and how is it implemented?** |
|  |

**Maintenance**

**MA-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] maintenance policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and

c. Review and update the current maintenance:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **MA-1 Control Summary Information** |
| Responsible Role: |
| Parameter MA-1(a): |
| Parameter MA-1(a)(1): |
| Parameter MA-1(b): |
| Parameter MA-1(c)(1)-1: |
| Parameter MA-1(c)(1)-2: |
| Parameter MA-1(c)(2)-1: |
| Parameter MA-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MA-1 What is the solution and how is it implemented?** |
|  |

**MA-2 Controlled Maintenance**

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

c. Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include the following information in organizational maintenance records: [Assignment: organization-defined information].

|  |
| --- |
| **MA-2 Control Summary Information** |
| Responsible Role: |
| Parameter MA-2(c): |
| Parameter MA-2(d): |
| Parameter MA-2(f): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MA-2 What is the solution and how is it implemented?** |
|  |

**MA-3 Maintenance Tools**

a. Approve, control, and monitor the use of system maintenance tools; and

b. Review previously approved system maintenance tools [Assignment: organization-defined frequency].

|  |
| --- |
| **MA-3 Control Summary Information** |
| Responsible Role: |
| Parameter MA-3(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MA-3 What is the solution and how is it implemented?** |
|  |

**MA-3(1) Inspect Tools**

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

|  |
| --- |
| **MA-3(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MA-3(1) What is the solution and how is it implemented?** |
|  |

**MA-3(2) Inspect Media**

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

|  |
| --- |
| **MA-3(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MA-3(2) What is the solution and how is it implemented?** |
|  |

**MA-3(3) Prevent Unauthorized Removal**

Prevent the removal of maintenance equipment containing organizational information by:

(a) Verifying that there is no organizational information contained on the equipment;

(b) Sanitizing or destroying the equipment;

(c) Retaining the equipment within the facility; or

(d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.

|  |
| --- |
| **MA-3(3) Control Summary Information** |
| Responsible Role: |
| Parameter MA-3(3)(d): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MA-3(3) What is the solution and how is it implemented?** |
|  |

**MA-4 Nonlocal Maintenance**

a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintain records for nonlocal maintenance and diagnostic activities; and

e. Terminate session and network connections when nonlocal maintenance is completed.

|  |
| --- |
| **MA-4 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MA-4 What is the solution and how is it implemented?** |
|  |

**MA-5 Maintenance Personnel**

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

|  |
| --- |
| **MA-5 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MA-5 What is the solution and how is it implemented?** |
|  |

**MA-5(1) Individuals Without Appropriate Access**

1. Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
2. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and
3. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

(b) Develop and implement [Assignment: organization-defined alternate controls] in the event a system component cannot be sanitized, removed, or disconnected from the system.

|  |
| --- |
| **MA-5(1) Control Summary Information** |
| Responsible Role: |
| Parameter MA-5(1)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MA-5(1) What is the solution and how is it implemented?** |
|  |

**MA-6 Timely Maintenance**

Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure.

|  |
| --- |
| **MA-6 Control Summary Information** |
| Responsible Role: |
| Parameter MA-6-1: |
| Parameter MA-6-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MA-6 What is the solution and how is it implemented?** |
|  |

**Media Protection**

**MP-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] media protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and

c. Review and update the current media protection:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **MP-1 Control Summary Information** |
| Responsible Role: |
| Parameter MP-1(a): |
| Parameter MP-1(a)(1): |
| Parameter MP-1(b): |
| Parameter MP-1(c)(1)-1: |
| Parameter MP-1(c)(1)-2: |
| Parameter MP-1(c)(2)-1: |
| Parameter MP-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MP-1 What is the solution and how is it implemented?** |
|  |

**MP-2 Media Access**

Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

|  |
| --- |
| **MP-2 Control Summary Information** |
| Responsible Role: |
| Parameter MP-2-1: |
| Parameter MP-2-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MP-2 What is the solution and how is it implemented?** |
|  |

**MP-3 Media Marking**

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas].

|  |
| --- |
| **MP-3 Control Summary Information** |
| Responsible Role: |
| Parameter MP-3(b)-1: |
| Parameter MP-3(b)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MP-3 What is the solution and how is it implemented?** |
|  |

**MP-4 Media Storage**

a. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and

b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

|  |
| --- |
| **MP-4 Control Summary Information** |
| Responsible Role: |
| Parameter MP-4(a)-1: |
| Parameter MP-4(a)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MP-4 What is the solution and how is it implemented?** |
|  |

**MP-5 Media Transport**

a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls];

b. Maintain accountability for system media during transport outside of controlled areas;

c. Document activities associated with the transport of system media; and

d. Restrict the activities associated with the transport of system media to authorized personnel.

|  |
| --- |
| **MP-5 Control Summary Information** |
| Responsible Role: |
| Parameter MP-5(a)-1: |
| Parameter MP-5(a)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MP-5 What is the solution and how is it implemented?** |
|  |

**MP-6 Media Sanitization**

a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

|  |
| --- |
| **MP-6 Control Summary Information** |
| Responsible Role: |
| Parameter MP-6(a)-1: |
| Parameter MP-6(a)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MP-6 What is the solution and how is it implemented?** |
|  |

**MP-7 Media Use**

a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and

b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

|  |
| --- |
| **MP-7 Control Summary Information** |
| Responsible Role: |
| Parameter MP-7(a)-1: |
| Parameter MP-7(a)-2: |
| Parameter MP-7(a)-3: |
| Parameter MP-7(a)-4: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **MP-7 What is the solution and how is it implemented?** |
|  |

**Physical and Environmental Protection**

**PE-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] physical and environmental protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **PE-1 Control Summary Information** |
| Responsible Role: |
| Parameter PE-1(a): |
| Parameter PE-1(a)(1): |
| Parameter PE-1(b): |
| Parameter PE-1(c)(1)-1: |
| Parameter PE-1(c)(1)-2: |
| Parameter PE-1(c)(2)-1: |
| Parameter PE-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-1 What is the solution and how is it implemented?** |
|  |

**PE-2 Physical Access Authorizations**

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and

d. Remove individuals from the facility access list when access is no longer required.

|  |
| --- |
| **PE-2 Control Summary Information** |
| Responsible Role: |
| Parameter PE-2(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-2 What is the solution and how is it implemented?** |
|  |

**PE-3 Physical Access Control**

a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by:

1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards];

b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points];

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls];

d. Escort visitors and control visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity];

e. Secure keys, combinations, and other physical access devices;

f. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and

g. Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

|  |
| --- |
| **PE-3 Control Summary Information** |
| Responsible Role: |
| Parameter PE-3(a): |
| Parameter PE-3(a)(2): |
| Parameter PE-3(b): |
| Parameter PE-3(c): |
| Parameter PE-3(d): |
| Parameter PE-3(f)-1: |
| Parameter PE-3(f)-2: |
| Parameter PE-3(g): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-3 What is the solution and how is it implemented?** |
|  |

**PE-4 Access Control for Transmission**

Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].

|  |
| --- |
| **PE-4 Control Summary Information** |
| Responsible Role: |
| Parameter PE-4-1: |
| Parameter PE-4-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-4 What is the solution and how is it implemented?** |
|  |

**PE-5 Access Control for Output Devices**

Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.

|  |
| --- |
| **PE-5 Control Summary Information** |
| Responsible Role: |
| Parameter PE-5: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-5 What is the solution and how is it implemented?** |
|  |

**PE-6 Monitoring Physical Access**

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events; and

c. Coordinate results of reviews and investigations with the organizational incident response capability.

|  |
| --- |
| **PE-6 Control Summary Information** |
| Responsible Role: |
| Parameter PE-6(b)-1: |
| Parameter PE-6(b)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-6 What is the solution and how is it implemented?** |
|  |

**PE-6(1) Intrusion Alarms and Surveillance Equipment**

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

|  |
| --- |
| **PE-6(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-6(1) What is the solution and how is it implemented?** |
|  |

**PE-8 Visitor Access Records**

a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period];

b. Review visitor access records [Assignment: organization-defined frequency]; and

c. Report anomalies in visitor access records to [Assignment: organization-defined personnel].

|  |
| --- |
| **PE-8 Control Summary Information** |
| Responsible Role: |
| Parameter PE-8(a): |
| Parameter PE-8(b): |
| Parameter PE-8(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-8 What is the solution and how is it implemented?** |
|  |

**PE-9 Power Equipment and Cabling**

Protect power equipment and power cabling for the system from damage and destruction.

|  |
| --- |
| **PE-9 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-9 What is the solution and how is it implemented?** |
|  |

**PE-10 Emergency Shutoff**

a. Provide the capability of shutting off power to [Assignment: organization-defined system or individual system components] in emergency situations;

b. Place emergency shutoff switches or devices in [Assignment: organization-defined location by system or system component] to facilitate access for authorized personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

|  |
| --- |
| **PE-10 Control Summary Information** |
| Responsible Role: |
| Parameter PE-10(a): |
| Parameter PE-10(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-10 What is the solution and how is it implemented?** |
|  |

**PE-11 Emergency Power**

Provide an uninterruptible power supply to facilitate [Selection (one or more): Assignment: an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.

|  |
| --- |
| **PE-11 Control Summary Information** |
| Responsible Role: |
| Parameter PE-11: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-11 What is the solution and how is it implemented?** |
|  |

**PE-12 Emergency Lighting**

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

|  |
| --- |
| **PE-12 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-12 What is the solution and how is it implemented?** |
|  |

**PE-13 Fire Protection**

Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

|  |
| --- |
| **PE-13 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-13 What is the solution and how is it implemented?** |
|  |

**PE-13(1) Detection Systems — Automatic Activation and Notification**

Employ fire detection systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.

|  |
| --- |
| **PE-13(1) Control Summary Information** |
| Responsible Role: |
| Parameter PE-13(1)-1: |
| Parameter PE-13(1)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-13(1) What is the solution and how is it implemented?** |
|  |

**PE-13(2) Suppression Systems — Automatic Activation and Notification**

(a) Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; and

(b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

|  |
| --- |
| **PE-13(2) Control Summary Information** |
| Responsible Role: |
| Parameter PE-13(2)(a)-1: |
| Parameter PE-13(2)(a)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-13(2) What is the solution and how is it implemented?** |
|  |

**PE-14 Environmental Controls**

a. Maintain [Selection (one or more): temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; and

b. Monitor environmental control levels [Assignment: organization-defined frequency].

|  |
| --- |
| **PE-14 Control Summary Information** |
| Responsible Role: |
| Parameter PE-14(a)-1: |
| Parameter PE-14(a)-2: |
| Parameter PE-14(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-14 What is the solution and how is it implemented?** |
|  |

**PE-15 Water Damage Protection**

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

|  |
| --- |
| **PE-15 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-15 What is the solution and how is it implemented?** |
|  |

**PE-16 Delivery and Removal**

a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; and

b. Maintain records of the system components.

|  |
| --- |
| **PE-16 Control Summary Information** |
| Responsible Role: |
| Parameter PE-16(a): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-16 What is the solution and how is it implemented?** |
|  |

**PE-17 Alternate Work Site**

a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees;

b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls];

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

|  |
| --- |
| **PE-17 Control Summary Information** |
| Responsible Role: |
| Parameter PE-17(a): |
| Parameter PE-17(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PE-17 What is the solution and how is it implemented?** |
|  |

**Planning**

**PL-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] planning policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and

c. Review and update the current planning:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **PL-1 Control Summary Information** |
| Responsible Role: |
| Parameter PL-1(a): |
| Parameter PL-1(a)(1): |
| Parameter PL-1(b): |
| Parameter PL-1(c)(1)-1: |
| Parameter PL-1(c)(1)-2: |
| Parameter PL-1(c)(2)-1: |
| Parameter PL-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PL-1 What is the solution and how is it implemented?** |
|  |

**PL-2 System Security and Privacy Plans**

a. Develop security and privacy plans for the system that:

1. Are consistent with the organization’s enterprise architecture;

2. Explicitly define the constituent system components;

3. Describe the operational context of the system in terms of mission and business processes;

4. Identify the individuals that fulfill system roles and responsibilities;

5. Identify the information types processed, stored, and transmitted by the system;

6. Provide the security categorization of the system, including supporting rationale;

7. Describe any specific threats to the system that are of concern to the organization;

8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

10. Provide an overview of the security and privacy requirements for the system;

11. Identify any relevant control baselines or overlays, if applicable;

12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;

13. Include risk determinations for security and privacy architecture and design decisions;

14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and

15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];

c. Review the plans [Assignment: organization-defined frequency];

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

|  |
| --- |
| **PL-2 Control Summary Information** |
| Responsible Role: |
| Parameter PL-2(a)(14): |
| Parameter PL-2(b): |
| Parameter PL-2(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PL-2 What is the solution and how is it implemented?** |
|  |

**PL-4 Rules of Behavior**

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;

c. Review and update the rules of behavior [Assignment: organization-defined frequency]; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].

|  |
| --- |
| **PL-4 Control Summary Information** |
| Responsible Role: |
| Parameter PL-4(c): |
| Parameter PL-4(d): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PL-4 What is the solution and how is it implemented?** |
|  |

**PL-4(1) Social Media and External Site/Application Usage Restrictions**

Include in the rules of behavior, restrictions on:

(a) Use of social media, social networking sites, and external sites/applications;

(b) Posting organizational information on public websites; and

(c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

|  |
| --- |
| **PL-4(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PL-4(1) What is the solution and how is it implemented?** |
|  |

**PL-8 Security and Privacy Architectures**

a. Develop security and privacy architectures for the system that:

1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;

2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;

3. Describe how the architectures are integrated into and support the enterprise architecture; and

4. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

|  |
| --- |
| **PL-8 Control Summary Information** |
| Responsible Role: |
| Parameter PL-8(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PL-8 What is the solution and how is it implemented?** |
|  |

**PL-10 Baseline Selection**

Select a control baseline for the system.

|  |
| --- |
| **PL-10 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PL-10 What is the solution and how is it implemented?** |
|  |

**PL-11 Baseline Tailoring**

Tailor the selected control baseline by applying specified tailoring actions.

|  |
| --- |
| **PL-11 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PL-11 What is the solution and how is it implemented?** |
|  |

**Personnel Security**

**PS-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] personnel security policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **PS-1 Control Summary Information** |
| Responsible Role: |
| Parameter PS-1(a): |
| Parameter PS-1(a)(1): |
| Parameter PS-1(b): |
| Parameter PS-1(c)(1)-1: |
| Parameter PS-1(c)(1)-2: |
| Parameter PS-1(c)(2)-1: |
| Parameter PS-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PS-1 What is the solution and how is it implemented?** |
|  |

**PS-2 Position Risk Designation**

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations [Assignment: organization-defined frequency].

|  |
| --- |
| **PS-2 Control Summary Information** |
| Responsible Role: |
| Parameter PS-2(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PS-2 What is the solution and how is it implemented?** |
|  |

**PS-3 Personnel Screening**

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].

|  |
| --- |
| **PS-3 Control Summary Information** |
| Responsible Role: |
| Parameter PS-3(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PS-3 What is the solution and how is it implemented?** |
|  |

**PS-3(3) Information Requiring Special Protective Measures**

Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:

(a) Have valid access authorizations that are demonstrated by assigned official government duties; and

(b) Satisfy [Assignment: organization-defined additional personnel screening criteria].

|  |
| --- |
| **PS-3(3) Control Summary Information** |
| Responsible Role: |
| Parameter PS-3(3)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PS-3(3) What is the solution and how is it implemented?** |
|  |

**PS-4 Personnel Termination**

Upon termination of individual employment:

a. Disable system access within [Assignment: organization-defined time period];

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics];

d. Retrieve all security-related organizational system-related property; and

e. Retain access to organizational information and systems formerly controlled by terminated individual.

|  |
| --- |
| **PS-4 Control Summary Information** |
| Responsible Role: |
| Parameter PS-4(a): |
| Parameter PS-4(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PS-4 What is the solution and how is it implemented?** |
|  |

**PS-5 Personnel Transfer**

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

|  |
| --- |
| **PS-5 Control Summary Information** |
| Responsible Role: |
| Parameter PS-5(b)-1: |
| Parameter PS-5(b)-2: |
| Parameter PS-5(d)-1: |
| Parameter PS-5(d)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PS-5 What is the solution and how is it implemented?** |
|  |

**PS-6 Access Agreements**

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements [Assignment: organization-defined frequency]; and

c. Verify that individuals requiring access to organizational information and systems:

1. Sign appropriate access agreements prior to being granted access; and

2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].

|  |
| --- |
| **PS-6 Control Summary Information** |
| Responsible Role: |
| Parameter PS-6(b): |
| Parameter PS-6(c)(2): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PS-6 What is the solution and how is it implemented?** |
|  |

**PS-7 External Personnel Security**

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time period]; and

e. Monitor provider compliance with personnel security requirements.

|  |
| --- |
| **PS-7 Control Summary Information** |
| Responsible Role: |
| Parameter PS-7(d)-1: |
| Parameter PS-7(d)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PS-7 What is the solution and how is it implemented?** |
|  |

**PS-8 Personnel Sanctions**

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and

b. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

|  |
| --- |
| **PS-8 Control Summary Information** |
| Responsible Role: |
| Parameter PS-8(b)-1: |
| Parameter PS-8(b)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PS-8 What is the solution and how is it implemented?** |
|  |

**PS-9 Position Descriptions**

Incorporate security and privacy roles and responsibilities into organizational position descriptions.

|  |
| --- |
| **PS-9 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **PS-9 What is the solution and how is it implemented?** |
|  |

**Risk Assessment**

**RA-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] risk assessment policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

c. Review and update the current risk assessment:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **RA-1 Control Summary Information** |
| Responsible Role: |
| Parameter RA-1(a): |
| Parameter RA-1(a)(1): |
| Parameter RA-1(b): |
| Parameter RA-1(c)(1)-1: |
| Parameter RA-1(c)(1)-2: |
| Parameter RA-1(c)(2)-1: |
| Parameter RA-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **RA-1 What is the solution and how is it implemented?** |
|  |

**RA-2 Security Categorization**

a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

|  |
| --- |
| **RA-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **RA-2 What is the solution and how is it implemented?** |
|  |

**RA-3 Risk Assessment**

a. Conduct a risk assessment, including:

1. Identifying threats to and vulnerabilities in the system;

2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]];

d. Review risk assessment results [Assignment: organization-defined frequency]];

e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and

f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

|  |
| --- |
| **RA-3 Control Summary Information** |
| Responsible Role: |
| Parameter RA-3(c): |
| Parameter RA-3(d): |
| Parameter RA-3(e): |
| Parameter RA-3(f): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **RA-3 What is the solution and how is it implemented?** |
|  |

**RA-3(1) Supply Chain Risk Assessment**

(a) Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; and

(b) Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in supply chain.

|  |
| --- |
| **RA-3(1) Control Summary Information** |
| Responsible Role: |
| Parameter RA-3(1)(a): |
| Parameter RA-3(1)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **RA-3(1) What is the solution and how is it implemented?** |
|  |

**RA-5 Vulnerability Monitoring and Scanning**

a. Monitor and scan for vulnerabilities in the system and hosted applications [[Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;

2. Formatting checklists and test procedures; and

3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

|  |
| --- |
| **RA-5 Control Summary Information** |
| Responsible Role: |
| Parameter RA-5(a): |
| Parameter RA-5(d): |
| Parameter RA-5(e): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **RA-5 What is the solution and how is it implemented?** |
|  |

**RA-5(2) Update Vulnerabilities to Be Scanned**

Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].

|  |
| --- |
| **RA-5(2) Control Summary Information** |
| Responsible Role: |
| Parameter RA-5(2): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **RA-5(2) What is the solution and how is it implemented?** |
|  |

**RA-5(3) Breadth and Depth of Coverage**

Define the breadth and depth of vulnerability scanning coverage.

|  |
| --- |
| **RA-5(3) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **RA-5(3) What is the solution and how is it implemented?** |
|  |

**RA-5(5) Privileged Access**

Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].

|  |
| --- |
| **RA-5(5) Control Summary Information** |
| Responsible Role: |
| Parameter RA-5(5)-1: |
| Parameter RA-5(5)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **RA-5(5) What is the solution and how is it implemented?** |
|  |

**RA-5(11) Public Disclosure Program**

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

|  |
| --- |
| **RA-5(11) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **RA-5(11) What is the solution and how is it implemented?** |
|  |

**RA-7 Risk Response**

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

|  |
| --- |
| **RA-7 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **RA-7 What is the solution and how is it implemented?** |
|  |

**RA-9 Criticality Analysis**

Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].

|  |
| --- |
| **RA-9 Control Summary Information** |
| Responsible Role: |
| Parameter RA-9-1: |
| Parameter RA-9-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **RA-9 What is the solution and how is it implemented?** |
|  |

**System and Services Acquisition**

**SA-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] system and services acquisition policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

c. Review and update the current system and services acquisition:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **SA-1 Control Summary Information** |
| Responsible Role: |
| Parameter SA-1(a): |
| Parameter SA-1(a)(1): |
| Parameter SA-1(b): |
| Parameter SA-1(c)(1)-1: |
| Parameter SA-1(c)(1)-2: |
| Parameter SA-1(c)(2)-1: |
| Parameter SA-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-1 What is the solution and how is it implemented?** |
|  |

**SA-2 Allocation of Resources**

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

|  |
| --- |
| **SA-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-2 What is the solution and how is it implemented?** |
|  |

**SA-3 System Development Life Cycle**

a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

|  |
| --- |
| **SA-3 Control Summary Information** |
| Responsible Role: |
| Parameter SA-3(a): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-3 What is the solution and how is it implemented?** |
|  |

**SA-4 Acquisition Process**

Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one-or-more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;

b. Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements.

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

|  |
| --- |
| **SA-4 Control Summary Information** |
| Responsible Role: |
| Parameter SA-4: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-4 What is the solution and how is it implemented?** |
|  |

**SA-4(1) Functional Properties of Controls**

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

|  |
| --- |
| **SA-4(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-4(1) What is the solution and how is it implemented?** |
|  |

**SA-4(2) Design and Implementation Information for Controls**

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].

|  |
| --- |
| **SA-4(2) Control Summary Information** |
| Responsible Role: |
| Parameter SA-4(2)-1: |
| Parameter SA-4(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-4(2) What is the solution and how is it implemented?** |
|  |

**SA-4(9) Functions, Ports, Protocols, and Services in Use**

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

|  |
| --- |
| **SA-4(9) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-4(9) What is the solution and how is it implemented?** |
|  |

**SA-4(10) Use of Approved PIV Products**

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

|  |
| --- |
| **SA-4(10) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-4(10) What is the solution and how is it implemented?** |
|  |

**SA-5 System Documentation**

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

1. Secure configuration, installation, and operation of the system, component, or service;

2. Effective use and maintenance of security and privacy functions and mechanisms; and

3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; and

d. Distribute documentation to [Assignment: organization-defined personnel or roles].

|  |
| --- |
| **SA-5 Control Summary Information** |
| Responsible Role: |
| Parameter SA-5(c): |
| Parameter SA-5(d): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-5 What is the solution and how is it implemented?** |
|  |

**SA-8 Security and Privacy Engineering Principles**

Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].

|  |
| --- |
| **SA-8 Control Summary Information** |
| Responsible Role: |
| Parameter SA-8: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-8 What is the solution and how is it implemented?** |
|  |

**SA-9 External System Services**

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls];

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].

|  |
| --- |
| **SA-9 Control Summary Information** |
| Responsible Role: |
| Parameter SA-9(a): |
| Parameter SA-9(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-9 What is the solution and how is it implemented?** |
|  |

**SA-9(1) Risk Assessments and Organizational Approvals**

(a) Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and

(b) Verify that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].

|  |
| --- |
| **SA-9(1) Control Summary Information** |
| Responsible Role: |
| Parameter SA-9(1)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-9(1) What is the solution and how is it implemented?** |
|  |

**SA-9(2) Identification of Functions, Ports, Protocols, and Services**

Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services].

|  |
| --- |
| **SA-9(2) Control Summary Information** |
| Responsible Role: |
| Parameter SA-9(2): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-9(2) What is the solution and how is it implemented?** |
|  |

**SA-9(5) Processing, Storage, and Service Location**

Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].

|  |
| --- |
| **SA-9(5) Control Summary Information** |
| Responsible Role: |
| Parameter SA-9(5)-1: |
| Parameter SA-9(5)-2: |
| Parameter SA-9(5)-3: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-9(5) What is the solution and how is it implemented?** |
|  |

**SA-10 Developer Configuration Management**

Require the developer of the system, system component, or system service to:

a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal];

b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

|  |
| --- |
| **SA-10 Control Summary Information** |
| Responsible Role: |
| Parameter SA-10(a): |
| Parameter SA-10(b): |
| Parameter SA-10(e): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-10 What is the solution and how is it implemented?** |
|  |

**SA-11 Developer Testing and Evaluation**

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

a. Develop and implement a plan for ongoing security and privacy assessments;

b. Perform [Selection (one-or-more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage];

c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during testing and evaluation.

|  |
| --- |
| **SA-11 Control Summary Information** |
| Responsible Role: |
| Parameter SA-11(b)-1: |
| Parameter SA-11(b)-2: |
| Parameter SA-11(b)-3: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-11 What is the solution and how is it implemented?** |
|  |

**SA-11(1) Static Code Analysis**

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

|  |
| --- |
| **SA-11(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-11(1) What is the solution and how is it implemented?** |
|  |

**SA-11(2) Threat Modeling and Vulnerability Analyses**

Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:

(a) Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];

(b) Employs the following tools and methods: [Assignment: organization-defined tools and methods];

(c) Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; and

(d) Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].

|  |
| --- |
| **SA-11(2) Control Summary Information** |
| Responsible Role: |
| Parameter SA-11(2)(a): |
| Parameter SA-11(2)(b): |
| Parameter SA-11(2)(c): |
| Parameter SA-11(2)(d): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-11(2) What is the solution and how is it implemented?** |
|  |

**SA-15 Development Process, Standards, and Tools**

a. Require the developer of the system, system component, or system service to follow a documented development process that:

1. Explicitly addresses security and privacy requirements;

2. Identifies the standards and tools used in the development process;

3. Documents the specific tool options and tool configurations used in the development process; and

4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements].

|  |
| --- |
| **SA-15 Control Summary Information** |
| Responsible Role: |
| Parameter SA-15(b)-1: |
| Parameter SA-15(b)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-15 What is the solution and how is it implemented?** |
|  |

**SA-15(3) Criticality Analysis**

Require the developer of the system, system component, or system service to perform a criticality analysis:

(a) At the following decision points in the system development life cycle: [Assignment: organization-defined decision points in the system development life cycle]; and

(b) At the following level of rigor: [Assignment: organization-defined breadth and depth of criticality analysis].

|  |
| --- |
| **SA-15(3) Control Summary Information** |
| Responsible Role: |
| Parameter SA-15(3)(a): |
| Parameter SA-15(3)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-15(3) What is the solution and how is it implemented?** |
|  |

**SA-22 Unsupported System Components**

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one-or-more): in-house support; [Assignment: organization-defined support from external providers]].

|  |
| --- |
| **SA-22 Control Summary Information** |
| Responsible Role: |
| Parameter SA-22(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SA-22 What is the solution and how is it implemented?** |
|  |

**System and Communications Protection**

**SC-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] system and communications protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

c. Review and update the current system and communications protection:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **SC-1 Control Summary Information** |
| Responsible Role: |
| Parameter SC-1(a): |
| Parameter SC-1(a)(1): |
| Parameter SC-1(b): |
| Parameter SC-1(c)(1)-1: |
| Parameter SC-1(c)(1)-2: |
| Parameter SC-1(c)(2)-1: |
| Parameter SC-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider) |
| **SC-1 What is the solution and how is it implemented?** |
|  |

**SC-2 Separation of System and User Functionality**

Separate user functionality, including user interface services, from system management functionality.

|  |
| --- |
| **SC-2 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-2 What is the solution and how is it implemented?** |
|  |

**SC-4 Information in Shared System Resources**

Prevent unauthorized and unintended information transfer via shared system resources.

|  |
| --- |
| **SC-4 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-4 What is the solution and how is it implemented?** |
|  |

**SC-5 Denial-of-service Protection**

a. [Selection: Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events] and;

b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].

|  |
| --- |
| **SC-5 Control Summary Information** |
| Responsible Role: |
| Parameter SC-5(a)-1: |
| Parameter SC-5(a)-2: |
| Parameter SC-5(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-5 What is the solution and how is it implemented?** |
|  |

**SC-7 Boundary Protection**

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

b. Implement subnetworks for publicly accessible system components that are [Selection: Assignment: physically; logically] separated from internal organizational networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

|  |
| --- |
| **SC-7 Control Summary Information** |
| Responsible Role: |
| Parameter SC-7(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-7 What is the solution and how is it implemented?** |
|  |

**SC-7(3) Access Points**

Limit the number of external network connections to the system.

|  |
| --- |
| **SC-7(3) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-7(3) What is the solution and how is it implemented?** |
|  |

**SC-7(4) External Telecommunications Services**

(a) Implement a managed interface for each external telecommunication service;

(b) Establish a traffic flow policy for each managed interface;

(c) Protect the confidentiality and integrity of the information being transmitted across each interface;

(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;

(e) Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need;

(f) Prevent unauthorized exchange of control plane traffic with external networks;

(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

(h) Filter unauthorized control plane traffic from external networks.

|  |
| --- |
| **SC-7(4) Control Summary Information** |
| Responsible Role: |
| Parameter SC-7(4)(e): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-7(4) What is the solution and how is it implemented?** |
|  |

**SC-7(5) Deny by Default — Allow by Exception**

Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]].

|  |
| --- |
| **SC-7(5) Control Summary Information** |
| Responsible Role: |
| Parameter SC-7(5): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-7(5) What is the solution and how is it implemented?** |
|  |

**SC-7(7) Split Tunneling for Remote Devices**

Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].

|  |
| --- |
| **SC-7(7) Control Summary Information** |
| Responsible Role: |
| Parameter SC-7(7): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-7(7) What is the solution and how is it implemented?** |
|  |

**SC-7(8) Route Traffic to Authenticated Proxy Servers**

Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.

|  |
| --- |
| **SC-7(8) Control Summary Information** |
| Responsible Role: |
| Parameter SC-7(8)-1: |
| Parameter SC-7(8)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-7(8) What is the solution and how is it implemented?** |
|  |

**SC-7(12) Host-based Protection**

Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components].

|  |
| --- |
| **SC-7(12) Control Summary Information** |
| Responsible Role: |
| Parameter SC-7(12)-1: |
| Parameter SC-7(12)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-7(12) What is the solution and how is it implemented?** |
|  |

**SC-7(18) Fail Secure**

Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

|  |
| --- |
| **SC-7(18) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-7(18) What is the solution and how is it implemented?** |
|  |

**SC-8 Transmission Confidentiality and Integrity**

Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.

|  |
| --- |
| **SC-8 Control Summary Information** |
| Responsible Role: |
| Parameter SC-8: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-8 What is the solution and how is it implemented?** |
|  |

**SC-8(1) Cryptographic Protection**

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

|  |
| --- |
| **SC-8(1) Control Summary Information** |
| Responsible Role: |
| Parameter SC-8(1): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-8(1) What is the solution and how is it implemented?** |
|  |

**SC-10 Network Disconnect**

Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

|  |
| --- |
| **SC-10 Control Summary Information** |
| Responsible Role: |
| Parameter SC-10: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-10 What is the solution and how is it implemented?** |
|  |

**SC-12 Cryptographic Key Establishment and Management**

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

|  |
| --- |
| **SC-12 Control Summary Information** |
| Responsible Role: |
| Parameter SC-12: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-12 What is the solution and how is it implemented?** |
|  |

**SC-13 Cryptographic Protection**

a. Determine the [Assignment: organization-defined cryptographic uses]; and

b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].

|  |
| --- |
| **SC-13 Control Summary Information** |
| Responsible Role: |
| Parameter SC-13(a): |
| Parameter SC-13(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-13 What is the solution and how is it implemented?** |
|  |

**SC-15 Collaborative Computing Devices and Applications**

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and

b. Provide an explicit indication of use to users physically present at the devices.

|  |
| --- |
| **SC-15 Control Summary Information** |
| Responsible Role: |
| Parameter SC-15(a): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-15 What is the solution and how is it implemented?** |
|  |

**SC-17 Public Key Infrastructure Certificates**

a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and

b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

|  |
| --- |
| **SC-17 Control Summary Information** |
| Responsible Role: |
| Parameter SC-17(a): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-17 What is the solution and how is it implemented?** |
|  |

**SC-18 Mobile Code**

a. Define acceptable and unacceptable mobile code and mobile code technologies; and

b. Authorize, monitor, and control the use of mobile code within the system.

|  |
| --- |
| **SC-18 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-18 What is the solution and how is it implemented?** |
|  |

**SC-20 Secure Name/Address Resolution Service (Authoritative Source)**

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

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

|  |
| --- |
| **SC-20 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-20 What is the solution and how is it implemented?** |
|  |

**SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)**

Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

|  |
| --- |
| **SC-21 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-21 What is the solution and how is it implemented?** |
|  |

**SC-22 Architecture and Provisioning for Name/Address Resolution Service**

Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

|  |
| --- |
| **SC-22 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-22 What is the solution and how is it implemented?** |
|  |

**SC-23 Session Authenticity**

Protect the authenticity of communications sessions.

|  |
| --- |
| **SC-23 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-23 What is the solution and how is it implemented?** |
|  |

**SC-28 Protection of Information at Rest**

Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

|  |
| --- |
| **SC-28 Control Summary Information** |
| Responsible Role: |
| Parameter SC-28-1: |
| Parameter SC-28-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-28 What is the solution and how is it implemented?** |
|  |

**SC-28(1) Cryptographic Protection**

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].

|  |
| --- |
| **SC-28(1) Control Summary Information** |
| Responsible Role: |
| Parameter SC-28(1)-1: |
| Parameter SC-28(1)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-28(1) What is the solution and how is it implemented?** |
|  |

**SC-39 Process Isolation**

Maintain a separate execution domain for each executing system process.

|  |
| --- |
| **SC-39 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-39 What is the solution and how is it implemented?** |
|  |

**SC-45 System Time Synchronization**

Synchronize system clocks within and between systems and system components.

|  |
| --- |
| **SC-45 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-45 What is the solution and how is it implemented?** |
|  |

**SC-45(1) Synchronization with Authoritative Time Source**

(a) Compare the internal system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and

(b) Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].

|  |
| --- |
| **SC-45(1) Control Summary Information** |
| Responsible Role: |
| Parameter SC-45(1)(a)-1: |
| Parameter SC-45(1)(a)-2: |
| Parameter SC-45(1)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SC-45(1) What is the solution and how is it implemented?** |
|  |

**System and Information Integrity**

**SI-1 Policy and Procedures**

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] system and information integrity policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **SI-1 Control Summary Information** |
| Responsible Role: |
| Parameter SI-1(a): |
| Parameter SI-1(a)(1): |
| Parameter SI-1(b): |
| Parameter SI-1(c)(1)-1: |
| Parameter SI-1(c)(1)-2: |
| Parameter SI-1(c)(2)-1: |
| Parameter SI-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-1 What is the solution and how is it implemented?** |
|  |

**SI-2 Flaw Remediation**

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

|  |
| --- |
| **SI-2 Control Summary Information** |
| Responsible Role: |
| Parameter SI-2(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-2 What is the solution and how is it implemented?** |
|  |

**SI-2(2) Automated Flaw Remediation Status**

Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency].

|  |
| --- |
| **SI-2(2) Control Summary Information** |
| Responsible Role: |
| Parameter SI-2(2)-1: |
| Parameter SI-2(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-2(2) What is the solution and how is it implemented?** |
|  |

**SI-2(3) Time to Remediate Flaws and Benchmarks for Corrective Actions**

(a) Measure the time between flaw identification and flaw remediation; and

(b) Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].

|  |
| --- |
| **SI-2(3) Control Summary Information** |
| Responsible Role: |
| Parameter SI-2(3)(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-2(3) What is the solution and how is it implemented?** |
|  |

**SI-3 Malicious Code Protection**

a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and

2. Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

|  |
| --- |
| **SI-3 Control Summary Information** |
| Responsible Role: |
| Parameter SI-3(a): |
| Parameter SI-3(c)(1)-1: |
| Parameter SI-3(c)(1)-2: |
| Parameter SI-3(c)(2)-1: |
| Parameter SI-3(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-3 What is the solution and how is it implemented?** |
|  |

**SI-4 System Monitoring**

a. Monitor the system to detect:

1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and

2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];

c. Invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the system to collect organization-determined essential information; and

2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one-or-more): as needed; [Assignment: organization-defined frequency]].

|  |
| --- |
| **SI-4 Control Summary Information** |
| Responsible Role: |
| Parameter SI-4(a)(1): |
| Parameter SI-4(b): |
| Parameter SI-4(g)-1: |
| Parameter SI-4(g)-2: |
| Parameter SI-4(g)-3: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-4 What is the solution and how is it implemented?** |
|  |

**SI-4(1) System-wide Intrusion Detection System**

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

|  |
| --- |
| **SI-4(1) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-4(1) What is the solution and how is it implemented?** |
|  |

**SI-4(2) Automated Tools and Mechanisms for Real-time Analysis**

Employ automated tools and mechanisms to support near real-time analysis of events.

|  |
| --- |
| **SI-4(2) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-4(2) What is the solution and how is it implemented?** |
|  |

**SI-4(4) Inbound and Outbound Communications Traffic**

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;

(b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

|  |
| --- |
| **SI-4(4) Control Summary Information** |
| Responsible Role: |
| Parameter SI-4(4)(b)-1: |
| Parameter SI-4(4)(b)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-4(4) What is the solution and how is it implemented?** |
|  |

**SI-4(5) System-generated Alerts**

Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].

|  |
| --- |
| **SI-4(5) Control Summary Information** |
| Responsible Role: |
| Parameter SI-4(5)-1: |
| Parameter SI-4(5)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-4(5) What is the solution and how is it implemented?** |
|  |

**SI-4(16) Correlate Monitoring Information**

Correlate information from monitoring tools and mechanisms employed throughout the system.

|  |
| --- |
| **SI-4(16) Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-4(16) What is the solution and how is it implemented?** |
|  |

**SI-4(18) Analyze Traffic and Covert Exfiltration**

Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system].

|  |
| --- |
| **SI-4(18) Control Summary Information** |
| Responsible Role: |
| Parameter SI-4(18): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-4(18) What is the solution and how is it implemented?** |
|  |

**SI-4(23) Host-based Devices**

Implement the following host-based monitoring mechanisms at [Assignment: organization-defined system components]: [Assignment: organization-defined host-based monitoring mechanisms].

|  |
| --- |
| **SI-4(23) Control Summary Information** |
| Responsible Role: |
| Parameter SI-4(23)-1: |
| Parameter SI-4(23)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-4(23) What is the solution and how is it implemented?** |
|  |

**SI-5 Security Alerts, Advisories, and Directives**

a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to: [Selection (one-or-more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and

d. Implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.

|  |
| --- |
| **SI-5 Control Summary Information** |
| Responsible Role: |
| Parameter SI-5(a): |
| Parameter SI-5(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-5 What is the solution and how is it implemented?** |
|  |

**SI-6 Security and Privacy Function Verification**

a. Verify the correct operation of [Assignment: organization-defined security and privacy functions];

b. Perform the verification of the functions specified in SI-6a [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]];

c. Alert [Assignment: organization-defined personnel or roles] to failed security and privacy verification tests; and

d. [Selection (one-or-more): Shut the system down; Restart the system; alternative actions(s)] when anomalies are discovered.

|  |
| --- |
| **SI-6 Control Summary Information** |
| Responsible Role: |
| Parameter SI-6(a): |
| Parameter SI-6(b): |
| Parameter SI-6(c): |
| Parameter SI-6(d): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-6 What is the solution and how is it implemented?** |
|  |

**SI-7 Software, Firmware, and Information Integrity**

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].

|  |
| --- |
| **SI-7 Control Summary Information** |
| Responsible Role: |
| Parameter SI-7(a): |
| Parameter SI-7(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-7 What is the solution and how is it implemented?** |
|  |

**SI-7(1) Integrity Checks**

Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one-or-more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].

|  |
| --- |
| **SI-7(1) Control Summary Information** |
| Responsible Role: |
| Parameter SI-7(1)-1: |
| Parameter SI-7(1)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-7(1) What is the solution and how is it implemented?** |
|  |

**SI-7(7) Integration of Detection and Response**

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].

|  |
| --- |
| **SI-7(7) Control Summary Information** |
| Responsible Role: |
| Parameter SI-7(7): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-7(7) What is the solution and how is it implemented?** |
|  |

**SI-8 Spam Protection**

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

|  |
| --- |
| **SI-8 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-8 What is the solution and how is it implemented?** |
|  |

**SI-8(2) Automatic Updates**

Automatically update spam protection mechanisms [Assignment: organization-defined frequency].

|  |
| --- |
| **SI-8(2) Control Summary Information** |
| Responsible Role: |
| Parameter SI-8(2): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-8(2) What is the solution and how is it implemented?** |
|  |

**SI-10 Information Input Validation**

Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].

|  |
| --- |
| **SI-10 Control Summary Information** |
| Responsible Role: |
| Parameter SI-10: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-10 What is the solution and how is it implemented?** |
|  |

**SI-11 Error Handling**

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to [Assignment: organization-defined personnel or roles].

|  |
| --- |
| **SI-11 Control Summary Information** |
| Responsible Role: |
| Parameter SI-11(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-11 What is the solution and how is it implemented?** |
|  |

**SI-12 Information Management and Retention**

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

|  |
| --- |
| **SI-12 Control Summary Information** |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-12 What is the solution and how is it implemented?** |
|  |

**SI-16 Memory Protection**

Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].

|  |
| --- |
| **SI-16 Control Summary Information** |
| Responsible Role: |
| Parameter SI-16: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SI-16 What is the solution and how is it implemented?** |
|  |

**Supply Chain Risk Management**

**SR-1 Policy and Procedures**

a. Develop, document, and disseminate to [FedRAMP Assignment: to include chief privacy and ISSO and/or similar role or designees]:

1. [Selection (one-or-more): organization-level; mission/business process-level; system-level] supply chain risk management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:

1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

|  |
| --- |
| **SR-1 Control Summary Information** |
| Responsible Role: |
| Parameter SR-1(a): |
| Parameter SR-1(a)(1): |
| Parameter SR-1(b): |
| Parameter SR-1(c)(1)-1: |
| Parameter SR-1(c)(1)-2: |
| Parameter SR-1(c)(2)-1: |
| Parameter SR-1(c)(2)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SR-1 What is the solution and how is it implemented?** |
|  |

**SR-2 Supply Chain Risk Management Plan**

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services [Assignment: organization-defined systems, system components, or system services]

b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

|  |
| --- |
| **SR-2 Control Summary Information** |
| Responsible Role: |
| Parameter SR-2(a): |
| Parameter SR-2(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SR-2 What is the solution and how is it implemented?** |
|  |

**SR-2(1) Establish SCRM Team**

Establish a supply chain risk management team consisting of [Assignment: organization-defined personnel, roles, and responsibilities] to lead and support the following SCRM activities: [Assignment: organization-defined supply chain risk management activities].

|  |
| --- |
| **SR-2(1) Control Summary Information** |
| Responsible Role: |
| Parameter SR-2(1)-1: |
| Parameter SR-2(1)-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SR-2(1) What is the solution and how is it implemented?** |
|  |

**SR-3 Supply Chain Controls and Processes**

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel];

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls]; and

c. Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan [Assignment: organization-defined document]].

|  |
| --- |
| **SR-3 Control Summary Information** |
| Responsible Role: |
| Parameter SR-3(a)-1: |
| Parameter SR-3(a)-2: |
| Parameter SR-3(b): |
| Parameter SR-3(c): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SR-3 What is the solution and how is it implemented?** |
|  |

**SR-5 Acquisition Strategies, Tools, and Methods**

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].

|  |
| --- |
| **SR-5 Control Summary Information** |
| Responsible Role: |
| Parameter SR-5: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SR-5 What is the solution and how is it implemented?** |
|  |

**SR-6 Supplier Assessments and Reviews**

Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].

|  |
| --- |
| **SR-6 Control Summary Information** |
| Responsible Role: |
| Parameter SR-6: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SR-6 What is the solution and how is it implemented?** |
|  |

**SR-8 Notification Agreements**

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]].

|  |
| --- |
| **SR-8 Control Summary Information** |
| Responsible Role: |
| Parameter SR-8: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SR-8 What is the solution and how is it implemented?** |
|  |

**SR-10 Inspection of Systems or Components**

Inspect the following systems or system components [Selection (one-or-more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].

|  |
| --- |
| **SR-10 Control Summary Information** |
| Responsible Role: |
| Parameter SR-10-1: |
| Parameter SR-10-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SR-10 What is the solution and how is it implemented?** |
|  |

**SR-11 Component Authenticity**

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to [Selection (one-or-more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].

|  |
| --- |
| **SR-11 Control Summary Information** |
| Responsible Role: |
| Parameter SR-11(b): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SR-11 What is the solution and how is it implemented?** |
|  |

**SR-11(1) Anti-counterfeit Training**

Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).

|  |
| --- |
| **SR-11(1) Control Summary Information** |
| Responsible Role: |
| Parameter SR-11(1): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SR-11(1) What is the solution and how is it implemented?** |
|  |

**SR-11(2) Configuration Control for Component Service and Repair**

Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [Assignment: organization-defined system components].

|  |
| --- |
| **SR-11(2) Control Summary Information** |
| Responsible Role: |
| Parameter SR-11(2): |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SR-11(2) What is the solution and how is it implemented?** |
|  |

**SR-12 Component Disposal**

Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].

|  |
| --- |
| **SR-12 Control Summary Information** |
| Responsible Role: |
| Parameter SR-12-1: |
| Parameter SR-12-2: |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative implementation  Not Applicable |
| Control Origination (check all that apply):  Cloud Service Provider  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited by Service Provider |
| **SR-12 What is the solution and how is it implemented?** |
|  |

# 

# SSP Required Appendices List

| Appendix Name | Filename |
| --- | --- |
| **Appendix C: Security Policies and Procedures** |  |
| **Appendix F: Rules of Behavior** |  |
| **Appendix G: Information System Contingency Plan (ISCP)** |  |
| **Appendix H: Configuration Management Plan (CMP)** |  |
| **Appendix I: Incident Response Plan (IRP)** |  |
| **Appendix K: System FIPS 199 Categorization Worksheet** |  |
| **Appendix N: Continuous Monitoring Plan** |  |
| **Appendix O: POA&M** |  |
| **Appendix P: Supply Chain Risk Management Plan (SCRMP)** |  |