|  |
| --- |
| FedRAMP System Security Plan (SSP)    Microsoft  Office 365 MT SSP  Version # 8.02  July 24, 2020 |



System Security Plan

Prepared by

|  |  |  |
| --- | --- | --- |
| **Identification of Organization that Prepared this Document** | | |
|  | Organization Name | First Information Technology Services, Inc. |
| Street Address | 777 108th Ave. NE |
| Suite/Room/Building | 1850 |
| City, State Zip | Bellevue, Washington 98004 |

Prepared for

|  |  |  |
| --- | --- | --- |
| **Identification of Cloud Service Provider** | | |
|  | Organization Name | Microsoft Corporation |
| Street Address | 1 Microsoft Way |
| Suite/Room/Building | Building 31 |
| City, State Zip | Redmond, WA 98052 |

Template Revision History

|  |  |
| --- | --- |
| **Date** | **Description** |
| 1/21/2013 | Original publication |
| 6/6/2014 | Major revision for SP800-53 Revision 4. Includes new template and formatting changes. |
| 6/6/2018 | Revised controls for language consistency and updated Attachment 3 |
| 6/20/2016 | Original publication |
| 10/21/2016 | Removed tables in Sec 15.12 FedRAMP Laws and Regulations  Removed revision history tables in all of Sec 15  Removed Acronyms - see FedRAMP Master Acronyms and Glossary resource document  Added PTA to Sec 15.4 PTA and PIA  Added E-Authentication to Sec 15.3  Added FIPs to Sec 15.10 FIPS 199  Changed Inventory instruction and guidance Section 10 and Attachment 13  Removed chapter numbers from Attachments  Removed 3 questions from Sec 2.3 E-Authentication Determination |
| 6/6/2017 | Updated logo |
| 8/28/2018 | Revised controls for language consistency, updated section 2.3 and Attachment 3, added guidance to SA -9, updated requirements in RA-5 |

Document Revision History

| Date | Description | Version of SSP | Author |
| --- | --- | --- | --- |
| 1/9/2015 | Minor changes for beginning of audit; began detailed change log going forward | 2.03 | FITS |
| 6/5/2015 | Adjusted for Changes made in MSFT Environment and audit results | 2.04 | FITS |
| 7/6/2015 | Updated Control Summary Information for controls with customer responsibility & minor edits | 2.05 | FITS |
| 8/3/2015 | Updated Control Implementation Details for controls based on POA&M updates, and additional minor edits | 2.06 | FITS |
| 8/4/2015 | Updated Control Implementation Details for controls based on POA&M updates, and additional minor edits | 2.07 | FITS |
| 8/11/2015 | Updated Control Implementation Details & minor edits | 2.08 | FITS |
| 9/8/2015 | Updated Control Summary Information for controls with customer responsibility & minor edits | 2.09 | FITS |
| 12/14/2015 | Major revision for annual assessment; updated system description and reviewed and updated all control implementations. | 3.00 | FITS |
| 5/13/2016 | Minor revision to incorporate updates from FY16 FedRAMP audit | 3.01 | FITS |
| 7/28/2016 | Minor revision to include updates from FY16 FedRAMP SAR | 3.02 | FITS |
| 2/21/2017 | Major revision for annual assessment; updated system description and reviewed and updated all control implementations. | 4.00 | FITS |
| 9/30/17 | - Major revision for Delta Audit: added Microsoft Teams (MSTeams), Object Store (OStore), and Outlook Mobile (OLM) as new workloads.  - Added Atlassian to section 11 for system interconnections, and all relevant controls.  - Removed Level 3 Communications from section 11 and all relevant controls. | 5.00 | FITS |
| 10/27/17 | Added DFDs for MS Teams, Object Store, and Outlook Mobile | 5.01 | FITS |
| 1/12/17 | Minor revisions to include updates from FY 17 Delta Audit | 5.02 | FITS |
| 3/16/2018 | Major revision for annual assessment; updated system description and reviewed and updated all control implementations. | 6.0 | Microsoft |
| 8/31/2018 | Updated for Spring 2018 SAR and minor edits | 6.01 | Microsoft |
| 3/11/2019 | Major revision for annual assessment; updated to new FedRAMP SSP template, updated system description and reviewed and updated all control implementations. | 7.0 | Microsoft |
| 7/30/2019 | Updated for Spring 2019 SAR and minor edits | 7.01 | Microsoft |
| 2/24/2020 | Major revision for annual assessment; reviewed system description and updated control implementations | 8.0 | Microsoft |
| 5/11/2020 | Major revision to align with FedRAMP High baseline | 8.01 | Microsoft |
| 7/24/2020 | Updated for Spring 2020 SAR and minor edits | 8.02 | Microsoft |

How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact [*info@FedRAMP.gov*](mailto:info@fedramp.gov)

For more information about the FedRAMP project, see [www.FedRAMP.gov](http://www.fedramp.gov)

TABLE OF CONTENTS

[1. Information System Name/Title 9](#_Toc46408620)

[2. Information System Categorization 9](#_Toc46408621)

[2.1 Information Types 9](#_Toc46408622)

[2.2 Security Objectives Categorization (FIPS 199) 11](#_Toc46408623)

[2.3 Digital Identity Determination 11](#_Toc46408624)

[3. Information System Owner 11](#_Toc46408625)

[4. Authorizing Officials 12](#_Toc46408626)

[5. Other Designated Contacts 12](#_Toc46408627)

[6. Assignment of Security Responsibility 13](#_Toc46408628)

[7. Information System Operational Status 14](#_Toc46408629)

[8. Information System Type 14](#_Toc46408630)

[8.1. Cloud Service Models 14](#_Toc46408631)

[8.2. Cloud Deployment Models 15](#_Toc46408632)

[8.3. Leveraged Authorizations 15](#_Toc46408633)

[9. General System Description 16](#_Toc46408634)

[9.1. System Function or Purpose 16](#_Toc46408635)

[9.1.1. Service Summary 16](#_Toc46408636)

[9.1.2. Security Overview 17](#_Toc46408637)

[9.1.3. Active Directory Federation Service (ADFS) 18](#_Toc46408638)

[9.1.4. Office 365 MT vs Office 365 GCC 18](#_Toc46408639)

[9.2. Information System Components and Boundaries 19](#_Toc46408640)

[9.2.1. Cosmos 21](#_Toc46408641)

[9.2.2. Geneva 22](#_Toc46408642)

[9.3. Types of Users 22](#_Toc46408643)

[9.4. Network Architecture 24](#_Toc46408644)

[9.5. Service Description 25](#_Toc46408645)

[9.5.1. Exchange Online (EXO) 25](#_Toc46408646)

[9.5.2. SharePoint Online (SPO) 26](#_Toc46408647)

[9.5.3. Skype for Business (SFB) 28](#_Toc46408648)

[9.5.4. Office Online (WAC) 29](#_Toc46408649)

[9.5.5. Office 365 Remote Access Service (ORAS) 31](#_Toc46408650)

[9.5.6. Information Protection (IP) 32](#_Toc46408651)

[9.5.7. Office 365 Suite User Experience (SUE) 34](#_Toc46408652)

[9.5.8. Office Service Infrastructure (OSI) 35](#_Toc46408653)

[9.5.9. Azure Active Directory (AAD) 36](#_Toc46408654)

[9.5.10. Microsoft Teams (MSTeams) 37](#_Toc46408655)

[9.5.11. Bing 38](#_Toc46408656)

[9.5.12. Activity Feed Service (AFS) 39](#_Toc46408657)

[9.5.13. Search Content Service (SCS) 41](#_Toc46408658)

[9.5.14. Office Intelligent Services (IS) 42](#_Toc46408659)

[9.5.15. Customer Insight and Analysis (CIA) 43](#_Toc46408660)

[9.5.16. Cloud Input Intelligence (CII) 45](#_Toc46408661)

[9.5.17. Live People Card 46](#_Toc46408662)

[9.5.18. Delve 48](#_Toc46408663)

[10. System Environment and Inventory 49](#_Toc46408664)

[10.1. Data Flow 49](#_Toc46408665)

[10.2. Ports, Protocols and Services 50](#_Toc46408666)

[11. System Interconnections 50](#_Toc46408667)

[12. Laws, Regulations, Standards and Guidance 51](#_Toc46408668)

[12.1. Applicable Laws and Regulations 51](#_Toc46408669)

[12.2. Applicable Standards and Guidance 51](#_Toc46408670)

[13. Minimum Security Controls 51](#_Toc46408671)

[13.1. Access Control (AC) 63](#_Toc46408672)

[13.2. Awareness and Training (AT) 149](#_Toc46408673)

[13.3. Audit and Accountability (AU) 159](#_Toc46408674)

[13.4. Security Assessment and Authorization (CA) 200](#_Toc46408675)

[13.5. Configuration Management (CM) 222](#_Toc46408676)

[13.6. Contingency Planning (CP) 266](#_Toc46408677)

[13.7. Identification and Authentication (IA) 305](#_Toc46408678)

[13.8. Incident Response (IR) 354](#_Toc46408679)

[13.9. Maintenance (MA) 388](#_Toc46408680)

[13.10. Media Protection (MP) 407](#_Toc46408681)

[13.11. Physical and Environmental Protection (PE) 421](#_Toc46408682)

[13.12. Planning (PL) 453](#_Toc46408683)

[13.13. Personnel Security (PS) 463](#_Toc46408684)

[13.14. Risk Assessment (RA) 485](#_Toc46408685)

[13.15. System and Services Acquisition (SA) 500](#_Toc46408686)

[13.16. System and Communications Protection (SC) 537](#_Toc46408687)

[13.17. System and Information Integrity (SI) 585](#_Toc46408688)

[14. Acronyms 633](#_Toc46408689)

[15. Attachments 634](#_Toc46408690)

[ATTACHMENT 1 - Information Security Policies and Procedures 635](#_Toc46408691)

[ATTACHMENT 2 - User Guide 635](#_Toc46408692)

[ATTACHMENT 3 - Digital Identity Worksheet 635](#_Toc46408693)

[Introduction and Purpose 635](#_Toc46408694)

[Information System Name/Title 635](#_Toc46408695)

[Digital Identity Level Definitions 636](#_Toc46408696)

[Review Maximum Potential Impact Levels 636](#_Toc46408697)

[Digital Identity Level Selection 637](#_Toc46408698)

[ATTACHMENT 4 - PTA / PIA 637](#_Toc46408699)

[Privacy Overview and Point of Contact (POC) 638](#_Toc46408700)

[Applicable Laws and Regulations 638](#_Toc46408701)

[Applicable Standards and Guidance 638](#_Toc46408702)

[Personally Identifiable Information (PII) 639](#_Toc46408703)

[Privacy Threshold Analysis 639](#_Toc46408704)

[Qualifying Questions 639](#_Toc46408705)

[Designation 640](#_Toc46408706)

[ATTACHMENT 5 - Rules of Behavior 640](#_Toc46408707)

[ATTACHMENT 6 - Information System Contingency Plan 641](#_Toc46408708)

[ATTACHMENT 7 - Configuration Management Plan 642](#_Toc46408709)

[ATTACHMENT 8 - Incident Response Plan 643](#_Toc46408710)

[ATTACHMENT 9 - CIS Workbook 644](#_Toc46408711)

[ATTACHMENT 10 - FIPS 199 645](#_Toc46408712)

[Introduction and Purpose 645](#_Toc46408713)

[Scope 645](#_Toc46408714)

[System Description 645](#_Toc46408715)

[Methodology 645](#_Toc46408716)

[ATTACHMENT 11 - Separation of Duties Matrix 647](#_Toc46408717)

[ATTACHMENT 12 - FedRAMP Laws and Regulations 648](#_Toc46408718)

[ATTACHMENT 13 - FedRAMP Inventory Workbook 648](#_Toc46408719)

[ATTACHMENT 14 – Ports, Protocols, and Services 649](#_Toc46408720)

[ATTACHMENT 15 – Office 365 Internal Documents 649](#_Toc46408721)

List of Figures

[Figure 9‑1. Network Diagram 15](#_Toc16580132)

[Figure 10‑1. Data Flow Diagram 38](#_Toc16580133)

List of Tables

[Table 1‑1. Information System Name and Title 1](#_Toc16579434)

[Table 2‑1. Security Categorization 1](#_Toc16579435)

[Table 2‑2. Sensitivity Categorization of Information Types 2](#_Toc16579436)

[Table 2‑3. Security Impact Level 3](#_Toc16579437)

[Table 2‑4. Baseline Security Configuration 3](#_Toc16579438)

[Table 3‑1. Information System Owner 4](#_Toc16579439)

[Table 5‑1. Information System Management Point of Contact 4](#_Toc16579440)

[Table 5‑2. Information System Technical Point of Contact 5](#_Toc16579441)

[Table 6‑1. Microsoft Internal ISSO (or Equivalent) Point of Contact 5](#_Toc16579442)

[Table 6‑2. AO Point of Contact 6](#_Toc16579443)

[Table 7‑1. System Status 6](#_Toc16579444)

[Table 8‑1. Service Layers Represented in this SSP 7](#_Toc16579445)

[Table 8‑2. Cloud Deployment Model Represented in this SSP 8](#_Toc16579446)

[Table 8‑3. Leveraged Authorizations 8](#_Toc16579447)

[Table 9‑1. Personnel Roles and Privileges 13](#_Toc16579448)

[Table 11‑1. System Interconnections 38](#_Toc16579449)

[Table 12‑1. Office 365 Laws and Regulations 40](#_Toc16579450)

[Table 12‑2. Office 365 Standards and Guidance 40](#_Toc16579451)

[Table 13‑1. Summary of Required Security Controls 41](#_Toc16579452)

[Table 13‑2. Control Origination and Definitions 46](#_Toc16579453)

[Table 13‑3. CA-3 Authorized Connections 173](#_Toc16579454)

[Table 15‑1. Names of Provided Attachments 578](#_Toc16579455)

[Table 15‑2. Information System Name and Title 579](#_Toc16579456)

[Table 15‑3. Mapping FedRAMP Levels to NIST SP 800-63-3 Levels 580](#_Toc16579457)

[Table 15‑4. Potential Impacts for Assurance Levels 581](#_Toc16579458)

[Table 15‑5. Digital Identity Level 581](#_Toc16579459)

[Table 15‑6. Office 365 Privacy POC 582](#_Toc16579460)

[Table 15‑7. Office 365 Laws and Regulations 583](#_Toc16579461)

[Table 15‑8. Office 365 Standards and Guidance 583](#_Toc16579462)

[Table 15‑9. CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1 592](#_Toc16579463)

[Table 15‑10. FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance 594](#_Toc16579464)

System Security Plan Approvals

Cloud Service Provider Signatures

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| Name | Greg Roberts | | Date |  |
| Title | Authorizing Official Microsoft | | | |
| Cloud Service Provider | | Microsoft | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | Shawn Veney | | Date |  |
| Title | Information System Security Officer | | | |
| Cloud Service Provider | | Microsoft | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name |  | | Date |  |
| Title |  | | | |
| Cloud Service Provider | |  | | |
|  | |  | | |

# Information System Name/Title

This System Security Plan provides an overview of the security requirements for Office 365 and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by Office 365.

The security safeguards implemented for the Office 365 system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table 1‑1. Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| MSO365MT | Office 365 MultiTenant | Office 365 MT |

# Information System Categorization

The overall information system sensitivity categorization is recorded in Table 2‑1. Security Categorization that follows. Directions for attaching the FIPS 199 document may be found in the following section: **Attachment 10. FIPS 199**.

Table 2‑1. Security Categorization

|  |  |
| --- | --- |
| System Sensitivity Level: | High (H) |

## Information Types

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

The following tables identify the information types that are input, stored, processed and/or output from Office 365. The selection of the information types is based on guidance provided by Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office Business Reference Model 2.0 and FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems which is based on NIST Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

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

The potential impact is low if—

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

The potential impact is moderate if—

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

The potential impact is high if—

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

Table 2‑2. Sensitivity Categorization of Information Types

| **Information Type**  **(Use only information types from NIST SP 800-60, Volumes I and II**  **as amended)** | **NIST 800-60 identifier for Associated Information Type** | **Confidentiality** | **Integrity** | **Availability** |
| --- | --- | --- | --- | --- |
| System Development | C.3.5.1 | Low (L) | Moderate (M) | Low (L) |
| Lifecycle/Change Management | C.3.5.2 | Low (L) | Moderate (M) | Low (L) |
| System Maintenance | C.3.5.3 | Low (L) | Moderate (M) | Low (L) |
| IT Infrastructure Maintenance | C.3.5.4 | Low (L) | Low (L) | Low (L) |
| Information Security | C.3.5.5 | Low (L) | Moderate (M) | Moderate (M) |
| Record Retention | C.3.5.6 | Low (L) | Low (L) | Low (L) |
| Information Management | C.3.5.7 | Low (L) | Moderate (M) | Low (L) |
| System and Network Monitoring | C.3.5.8 | Moderate (M) | Moderate (M) | Low (L) |
| Information Sharing | C.3.5.9 | Low (L) | Low (L) | Moderate (M) |

## Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2‑2. Sensitivity Categorization of Information Types, for Office 365, default to the high-water mark for the Information Types as identified in Table 2‑3. Security Impact Level below

.

Table 2‑3. Security Impact Level

| Security Objective | Low, Moderate or High |
| --- | --- |
| Confidentiality | High (H) |
| Integrity | High (H) |
| Availability | High (H) |

Through review and analysis, it has been determined that the baseline security categorization for Office 365 system is listed in the Table 2‑4. Baseline Security Configuration that follows.

Table 2‑4. Baseline Security Configuration

|  |  |
| --- | --- |
| Office 365 Security Categorization | High (H) |

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

## Digital Identity Determination

The digital identity information may be found in Attachment 3, Digital Identity Worksheet.

Note: NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

The digital identity level is Level 3: AAL3, IAL3, FAL3

# Information System Owner

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

Table 3‑1. Information System Owner

| Information System Owner Information | |
| --- | --- |
| * Name | Greg Roberts |
| * Title | Microsoft Office 365 Principal Group Program Manager |
| * Company / Organization | Microsoft / Office 365 |
| * Address | 1 Microsoft Way, Redmond, WA |
| * Phone Number | +1 (425) 722-6538 |
| * Email Address | groberts@microsoft.com |

# Authorizing Officials

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the FedRAMP PMO and Agency AO.

# Other Designated Contacts

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

Table 5‑1. Information System Management Point of Contact

| Information System Management Point of Contact | |
| --- | --- |
| Name | Melodi Crowley |
| Title | Principal Program Manager |
| Company / Organization | Microsoft / Office 365 Foundation |
| Address | 1 Microsoft Way, Redmond, WA 980521 |
| Phone Number | +1 (425) 722-8363 |
| Email Address | mcrowley@microsoft.com |

| Information System Management Point of Contact | |
| --- | --- |
| Name | Brittany Smith |
| Title | Sr. Program Manager |
| Company / Organization | Microsoft / Office 365 Foundation |
| Address | 1 Microsoft Way, Redmond, WA 980521 |
| Phone Number | +1 (425) 705-4258 |
| Email Address | Brittany.Smith@microsoft.com |

Table 5‑2. Information System Technical Point of Contact

| **Information System Technical Point of Contact** | |
| --- | --- |
| Name | Shawn Veney |
| Title | O365 Principal Architect |
| Company / Organization | Microsoft/ Office 365 Foundation |
| Address | 1 Microsoft Way, Redmond, WA 98052 |
| Phone Number | +1 (425) 706--9386 |
| Email Address | shawnven@microsoft.com |

| Point of Contact | |
| --- | --- |
| Name | Brittany Smith |
| Title | Sr. Program Manager |
| Company / Organization | Microsoft / Office 365 Foundation |
| Address | 1 Microsoft Way, Redmond, WA 980521 |
| Phone Number | +1 (425) 705-4258 |
| Email Address | Brittany.Smith@microsoft.com |

# Assignment of Security Responsibility

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

Table 6‑1. Microsoft Internal ISSO (or Equivalent) Point of Contact

| **Microsoft Internal ISSO (or Equivalent) Point of Contact** | |
| --- | --- |
| Name | Shawn Veney |
| Title | O365 Principal Architect |
| Company / Organization | Microsoft/ Office 365 Foundation |
| Address | 1 Microsoft Way, Redmond, WA 98052 |
| Phone Number | +1 (425) 706--9386 |
| Email Address | shawnven@microsoft.com |

Table 6‑2. AO Point of Contact

| AO Point of Contact | |
| --- | --- |
| Name | N/A |
| Title | N/A |
| Organization | N/A |
| Address | N/A |
| Phone Number | N/A |
| Email Address | N/A |

# Information System Operational Status

The system is currently in the life-cycle phase shown in Table 7‑1. System Status that follows. (Only operational systems can be granted an ATO).

Table 7‑1. System Status

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

# Information System Type

Office 365 makes use of unique managed service provider architecture layer(s).

## Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Below are some questions that help the system owner determine if their system is a cloud followed by specific questions to help the system owner determine the type of cloud.

| **Question (Yes/No)** | **Conclusion** |
| --- | --- |
| Does the system use virtual machines? | A no response means that system is most likely not a cloud. |
| Does the system have the ability to expand its capacity to meet customer demand? | A no response means that the system is most likely not a cloud. |
| Does the system allow the consumer to build anything other than servers? | A no response means that the system is an IaaS. A yes response means that the system is either a PaaS or a SaaS. |
| Does the system offer the ability to create databases? | A yes response means that the system is a PaaS. |
| Does the system offer various developer toolkits and APIs? | A yes response means that the system is a PaaS. |
| Does the system offer only applications that are available by obtaining a login? | A yes response means that system is a SaaS. A no response means that the system is either a PaaS or an IaaS. |

The layers of Office 365 defined in this SSP are indicated in Table 8‑1. Service Layers Represented in this SSP that follows.

Table 8‑1. Service Layers Represented in this SSP

| **Service Provider Architecture Layers** | | |
| --- | --- | --- |
| ☒ | Software as a Service (SaaS) | Major Application |
| ☐ | Platform as a Service (PaaS) | Major Application |
| ☐ | Infrastructure as a Service (IaaS) | General Support System |
| ☐ | Other | Explain: |

Note: Refer to NIST SP 800-145 for information on cloud computing architecture models.

## Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of Office 365 that are defined in this SSP and are not leveraged by any other FedRAMP Authorizations, are indicated in Table 8‑2. Cloud Deployment Model Represented in this SSP that follows.

| **Service Provider Cloud Deployment Model** | | |
| --- | --- | --- |
| ☒ | Public | Cloud services and infrastructure supporting multiple organizations and agency clients |
| ☐ | Private | Cloud services and infrastructure dedicated to a specific organization/agency and no other clients |
| ☐ | Government Only Community | Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations |
| ☐ | Hybrid | Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) |

Table 8‑2. Cloud Deployment Model Represented in this SS

## Leveraged Authorizations

Office 365 plans to leverage a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by Office 365 are listed in Table 8‑3. Leveraged Authorizations that follows.

Table 8‑3. Leveraged Authorizations

| **Leveraged Information System Name** | **Leveraged Service Provider Owner** | **Date Granted** |
| --- | --- | --- |
| Microsoft Azure Commercial Cloud Solution (F1209051525) | Microsoft | 5/3/2019 |
| Akamai Content Delivery Services (F1206061353) | Akamai | 8/23/2013 |

# General System Description

This section includes a general description of Office 365.

## System Function or Purpose

This service overview focuses on providing the background necessary to understand the implementation details in section 13 of this SSP. Section 9.1 provides a brief discussion of the customer-facing features and functionality of Office 365. Section 9.2, 9.3 and 9.4 provide a high-level overview of the security components, boundary, users and architecture of Office 365. Section 9.5 provides a summary of each component of Office 365 explaining how that component fits within the Office 365 security architecture.

### Service Summary

Office 365 is a multi-tenant cloud computing-based subscription service offering from Microsoft. Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. Further, as defined within NIST SP 800-145 (The NIST Definition of Cloud Computing), the service model for Office 365 is Software-as-a-Service (SaaS). SaaS is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

Office 365 provides customers with cloud versions of Exchange Online (EXO), SharePoint Online (SPO) (including Access Online Project Online, and OneDrive for Business), Skype for Business (SFB), Information Protection (IP), Office Online (WAC), Office 365 Suite User Experience (SUE), Bing, Microsoft Teams (MSTeams), Delve and Customer Insight and Analysis (CIA). Detailed service descriptions for each service team are included in section 9.5 of this SSP.

Office 365 has a number of supporting services in addition to these core, customer-facing services: O365 Remote Access Service (ORAS), Office Service Infrastructure (OSI), Activity Feed Service (AFS), Search Content Service (SCS), Office Intelligent Services (IS), Bing, Loki and Cloud Input Intelligence (CII). Each core and supporting service is supported by a unique group of developers, testers, and administrators referred to throughout this document as a “service team.” Each service is deployed onto service-specific servers, whether physical or virtual. While each service team follows Microsoft O365 policy, their services may have unique implementations of some security controls. For this reason, the SSP provides unique answers for each service where necessary. Where services have identical implementations, the implementation details are combined. A description of each service, including an explanation of that service team’s high-level architecture is provided in section 9.5 of this SSP.

### Security Overview

Office 365 security and compliance is managed by a team named Office 365 Trust. Office 365 Trust ensures that all services comply with security controls, manages audits, writes and enforces Microsoft policy, manages POA&Ms, and manages FedRAMP continuous monitoring. Please see the applicable controls from section 13 of this SSP for details on implementations of these responsibilities. Incident Response is managed for all service teams by the Office 365 Security Incident & Response team (SIR); details can be found in the Incident Response controls in section 13 of this SSP. Contingency and continuity planning are managed by the “Business Continuity Management Team” (BCM) in coordination with Office 365 Trust; details can be found in the Contingency Planning controls in section 13 of this SSP.

All Office 365 services are hosted on Microsoft Azure IaaS/PaaS product, which has a FedRAMP P-ATO. In this case, the physical servers are owned by Office 365, the operating system and software are managed by Office 365, and network layer and network layer protections are implemented by Azure. The configuration of the network layer/protection is managed by Office 365 in coordination with Azure. Azure is responsible for physical and environmental security. These servers are located in continental United States (CONUS) data centers as described in the Azure SSP. Details of Office 365 service teams are hosted on Azure are located in section 9.5 of this SSP.

Implementation of network layer security controls between the public internet and Office 365 is inherited from Azure. In all cases, there is a default deny-all policy for inbound traffic; only the specific ports and protocols required for the operation of the service and listed in Attachment 14 - Ports, Protocols and Services of this SSP are allowed. All traffic leaving the Office 365 boundary is encrypted and restricted as discussed primarily in the System and Communications Protection control family of this SSP. Section 10.1 has a detailed discussion of data flows crossing the Office 365 accreditation boundary.

Office 365 was built from the ground up as a multitenant cloud solution, considering the benefits and risks associated with that architecture. Microsoft designed Office 365 with the assumption that tenants of the system may be hostile and built in protections to ensure that tenants of Office 365 do not pose a risk to each other. Office 365 offers customers the scalability and cost savings of a multitenant cloud while preventing a weak security implementation by impacting the security of Office 365 or another Office 365 tenant.

Office 365 was designed using the principles of defense in depth. Cross tenant protections are implemented at the application layer to ensure that customers cannot compromise Office 365 applications to gain unauthorized access to the information of other tenants. Protections are also implemented at the network layer to prevent interception of network traffic and resource starvation attacks. Protections are additionally implemented at the operating system layer to prevent side channel attacks. Details regarding the protections implemented to prevent cross-tenant attacks are documented in “Tenant Isolation in Office 365.”

### Active Directory Federation Service (ADFS)

Microsoft requires that Government customers of Office 365 use Active Directory Federation Services (ADFS) for user provisioning, identity management, authentication, and permissions management. ADFS allows customers to maintain control of user identification and authentication from within their network and operating environment when using Office 365.

The implementation of ADFS creates a one-way trust from Office 365 to the customer’s existing AD infrastructure. When a Federal user attempts to access Office 365, the user is redirected to a login page that is hosted on the customer’s ADFS server. The user provides their credentials to this ADFS server, which validates them using the customer’s existing AD infrastructure. If the credentials are validated, the customer’s ADFS server issues a SAML ticket containing information about the user’s identity and group membership. The customer ADFS server signs this ticket using one half of an asymmetric key pair and the user sends the ticket to Office 365 via encrypted TLS 1.2. Office 365 validates the signature using the other half of the asymmetric key pair and grants access based on the ticket.

The use of ADFS requires directory synchronization between Office 365 and the customer’s ADFS server for user provisioning and de-provisioning. This synchronization occurs over a mutually authenticated encrypted TLS 1.2 connection. Additional information about the process of deploying ADFS and directory synchronization can be found at:

<http://technet.microsoft.com/en-us/library/jj205462.aspx>

Use of ADFS is required for FedRAMP-compliant use of Office 365; for details of how non-government customers who do not use ADFS authenticate, please see section 9.5.11 of this SSP. Use of ADFS means that the customer retains full or partial responsibility for many security controls, particularly within the Access Control (AC) and Identification and Authentication (IA) control families. Information about how the ADFS requirement affects specific security controls is provided with the relevant controls in section 13 of this SSP.

### Office 365 MT vs Office 365 GCC

Microsoft Office 365 MT meets FedRAMP requirements at data centers within the Continental US. Microsoft is aware that some Federal customers have additional security requirements beyond those specified by FedRAMP. One frequent requirement is that Microsoft administrators with logical access to customer content are U.S. citizens and undergo additional background screening. To meet this requirement, Microsoft offers an enhanced version of the O365 MT product which is marketed as ‘Office 365 Government Community Cloud’ (O365 GCC). Microsoft administrators with logical access to customer content stored or cached in O365 GCC are subject to these additional citizenship requirements and background screening. As a measure to further isolate services that store customer content, O365 GCC Exchange (EXO), O365 GCC Information Protection (IP), O365 GCC SharePoint (SPO), O365 GCC Skype for Business (SFB), and O365 GCC Microsoft Teams (MSTeams) are deployed to servers dedicated to U.S. Federal, State, and Local government customers.

A picture containing computer

Description automatically generated

Figure 9‑1. Office 365 MT and Office 365 GCC Separation Diagram

## Information System Components and Boundaries

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9‑2 Authorization Boundary Diagram below.



Figure 9‑2 Authorization Boundary Diagram

As discussed in section 9.1, Office 365 MT is a major application that provides hosted Exchange Online, SharePoint Online, and Skype for Business services. The Office 365 MT FedRAMP boundary includes these services, as well as many other services that support these core, customer-facing services. A detailed description of each in-boundary service is included in section 9.5 of this SSP. Each service outside the boundary is described below. Interconnections with external services are protected via Interconnection Security Agreements (ISA); each agreement details the requirements necessary to protect the connection and the data shared via that connection equivalently to the protections within Office 365 MT; a brief summary of these protections is listed here.

**Azure** contains services used by Office 365 MT to host various aspects of the Office 365 MT service. Connections to Azure services happen over FIPS 140-2 compatible TLS on specifically approved ports and protocols documented in ATTACHMENT 14 – Ports, Protocols and Services. These connections traverse the Azure network infrastructure where default-deny policies and other network protections are enforced. Specific controls inherited from Azure are listed in the Azure ISA. Azure has been granted a FedRAMP P-ATO.

**Akamai** represents the Global Traffic Manager (GTM) and Content Delivery Network (CDN) services run by Akamai Corporation on behalf of Office 365 MT. Akamai is used to distribute Office client software to end users. This use is protected via ISA with Akamai. No customer content is transmitted to Akamai or via Akamai. Interaction with this service is via API; the use of the API was developed in accordance with the Microsoft SDL process, which ensures that Office 365 MT does not rely on the external provider for security. Connections to Akamai happen over FIPS 140-2 compatible TLS on specifically approved ports and protocols documented in ATTACHMENT 14 – Ports, Protocols and Services. These connections traverse the Azure network infrastructure where default-deny policies and other network protections are enforced. No security controls are directly inherited from Akamai. Akamai has been granted a FedRAMP P-ATO.

**CorpNet** is a domain that contains services run on Microsoft’s corporate network, not dedicated to Office 365 MT, such as source code repositories, system documentation repositories, and change ticketing. No customer content is transmitted, processed or stored by CorpNet. Connections to these services happen via FIPS 140-2 compatible TLS on specifically approved ports and protocols documented in ATTACHMENT 14 – Ports, Protocols and Services. These connections traverse the Azure network infrastructure where default-deny policies and other network protections are enforced. No security controls are directly inherited from CorpNet.

TheSFB **PSTN** features require connectivity to the PSTN infrastructure to allow interaction between SFB and the PSTN. The Office 365 MT compliance boundary for PSTN features stops at the point where traffic is handed off to a PSTN carrier.

The Microsoft **Commerce** platform (Universal Store) manages direct customer communication and billing for Office 365. AAD pushes information to Commerce to facilitate billing and marketing for commercial clients. Only information necessary to facilitate billing and marketing is pushed to commerce; no other customer content is transmitted, processed, or stored by Commerce. Federal clients are billed through a separate solution and are not directly marketed to by the Microsoft Commerce division; federal customer information is deleted by the Commerce data collection process. These connections are shown for completeness. Connections to Commerce happen over FIPS 140-2 compatible TLS on specifically approved ports and protocols documented in ATTACHMENT 14 – Ports, Protocols and Services. Connections to these services happen via FIPS 140-2 compatible TLS on specifically approved ports and protocols documented in ATTACHMENT 14 – Ports, Protocols and Services. These connections traverse the Azure network infrastructure where default-deny policies and other network protections are enforced. No security controls are directly inherited from Commerce.

There is a connection between Office 365 Dedicated (a version of Office 365 not included in the accreditation boundary) and Office 365 MT. This connection exists so that Office 365 Dedicated can utilize certain Office 365 MT management servers. Information flow controls are in place to prevent the flow of any Office 365 MT data to Office 365 Dedicated and Office 365 MT does not depend on any controls implemented outside of Office 365 MT to maintain the confidentiality, integrity, and availability of Office 365 MT data with regard to this connection. This connection is documented here for completeness.

### Cosmos

Cosmos is a Microsoft service, not dedicated to Office 365 MT, that stores and reports on Office 365 log data. Office 365 scrubs logs of customer content before sending logs to Cosmos. Specifically, scrubbing takes fields containing customer content, encrypts or hashes that data, and replaces the field with the encrypted or hashed value. The rewritten log is sent to Cosmos, while each service team stores encryption keys and a mapping of hash keys to hashes within the Office 365 accreditation boundary. Cosmos can then correlate, alert, and report on these anonymized hashes. If an alert or report requires investigation, the logs are imported back inside the boundary. The service team can then repopulate the logs to their original state using the hash to key mapping. Because of the important nature of the Cosmos service, even though it does not store or process any customer content, it is expected that Cosmos security pertaining to protecting Office 365 will be assessed directly as part of FedRAMP accreditation auditing. Connections to Cosmos happen over FIPS 140-2 compatible TLS on specifically approved ports and protocols documented in ATTACHMENT 14 – Ports, Protocols and Services. These connections traverse the Azure network infrastructure where default-deny policies and other network protections are enforced.

### Geneva

Geneva is an extensible collection of libraries, tools and services that enable services to do Monitoring, Diagnostics and Analytics at scale. It is designed to support the requirements of all internal cloud services available on Azure and PilotFish environments. The Geneva System is part of the Cloud Engineering Services (CloudES) suite and active monitoring is offered to allow teams to build rich alerting. Geneva is a fully compliant offering (Azure and Office 365) and available in all national clouds.

## Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 9‑1. Personnel Roles and Privileges that follows.

Table 9‑1. Personnel Roles and Privileges

| Role | Internal or External | Privileged (P), Non-Privileged (NP), or No Logical Access (NLA) | Sensitivity Level | Authorized Privileges | Functions Performed |
| --- | --- | --- | --- | --- | --- |
| Customer User | External | N/A | N/A | N/A | Access Office 365 MT services |
| Customer Administrator | External | N/A | Limited | Customer portal administration | Administer customer user accounts, modify Office 365 MT service configurations |
| Service Engineer Operations | Internal | P | High-Risk | MT service production administrative access | Administer production Office 365 MT service |
| Program Manager | Internal | P | Moderate | Service team administrative access | Manages service team compliance |
| Developer | Internal | P | Moderate | Service team development environment access | Develops Office 365 MT |
| Tester | Internal | P | Moderate | Service team testing environment access | Tests Office 365 MT |
| Trust Program Manager | Internal | P | Limited | N/A | Responsible for compliance across all service teams, maintains compliance documentation |
| Office 365 Security Manager | Internal | P | Limited | N/A | Provides security governance and services, including vulnerability scanning, identity management, security incident response, audit collection and anti-virus and services, including vulnerability scanning, identity management, security incident response, audit collection and anti-virus |

The count of current users is proprietary information that is owned by Microsoft. The forecast of expected future customer users and internal administrators is proprietary information that is owned by Microsoft.

## Network Architecture

The following Figure 9‑2 Network Diagram provides a visual depiction of how Office 365 MT integrates into the Azure network architecture.



Figure 9‑2 Network Diagram

Office 365 MT leverages Azure for network infrastructure support, Data Center hosting, network operations, and physical/environmental controls. The Azure system accreditation boundary for FedRAMP consists of the Azure-managed domestic Data Centers (as outlined in the Azure SSP), the Azure core network infrastructure, the core servers providing critical shared services and management tools for the infrastructure, and the access network infrastructure that supports these critical core services. Office 365 MT servers are deployed into the area marked “Office 365 Authorization Boundary” on the bottom left of figure 9-2. These servers benefit from the same network protections and infrastructure as Azure’s core critical servers and Azure.

A complete listing of the Azure servers and network devices included in the Azure Accreditation Boundary can be found in the Azure Assessment & Authorization.



## Service Description

A summary of the security environment for each service team is provided below, along with a service-team view of the data flows. An explanation of the full data flow can be found in section 9.2. Implementation details for all controls are found in section 13 of this SSP. The summaries in this section are intended to help the reader better understand the section 13 implementation details by providing background and context.

### Exchange Online (EXO)

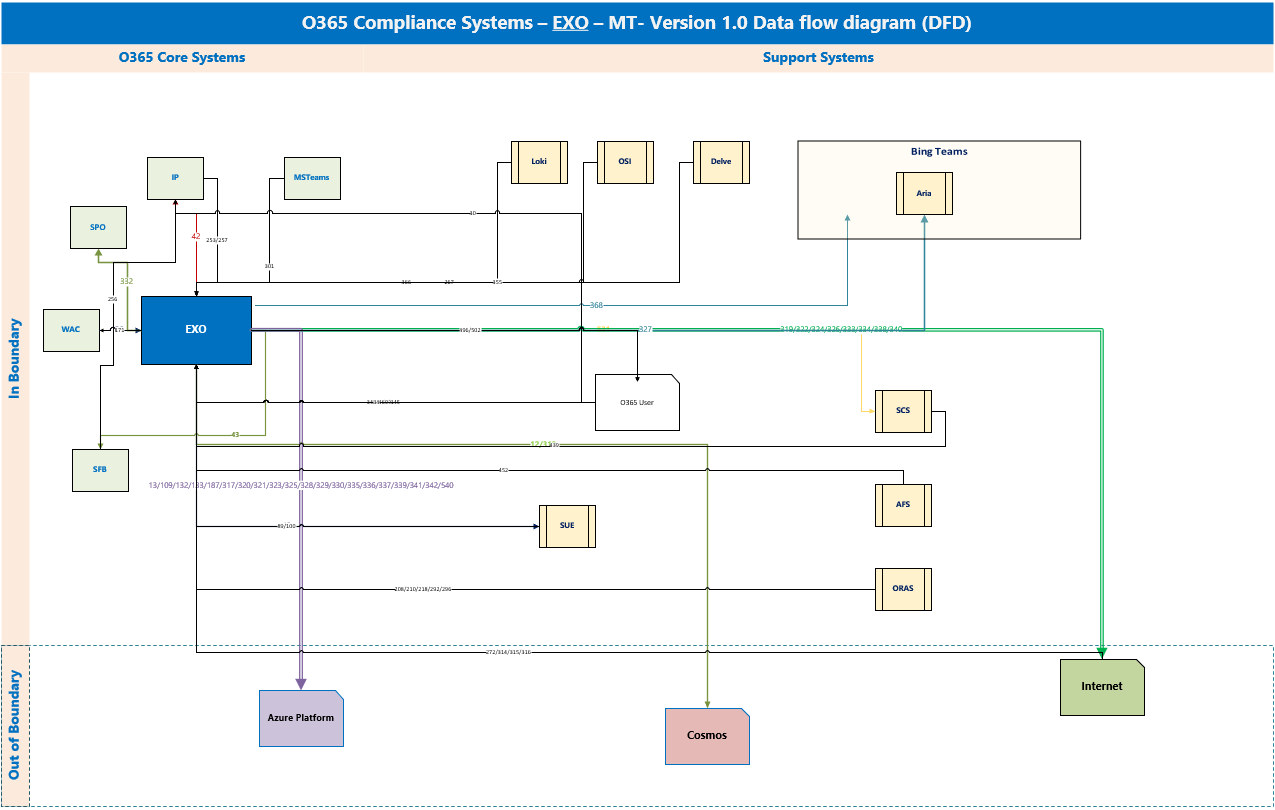


Figure 9‑3 Exchange Online Data Flows

Exchange Online (EXO) allows customers to access business email, calendar, and contacts on workstations, phones, and web browsers. The Exchange admin center provides an easy-to-use, web-based interface to manage their email services. Additionally, MyAnalytics on EXO helps customers build better work habits with personal productivity analytics.

EXO is hosted on physical servers within Azure CONUS data centers. These servers are joined to a security domain managed by EXO. Network access to these servers is controlled by Azure-owned and managed network devices using rules managed by EXO and approved by Office 365. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between EXO servers and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators access EXO through remote desktop gateways managed by the Office 365 Remote Access Service (ORAS); this access requires YubiKey-based multifactor authentication.

Users interact with EXO via software email clients (e.g. Outlook) and webmail. Users’ access to customer content is based on claims information contained in tickets issued by AAD. The user authenticates to their own ADFS infrastructure (as explained in section 9.1.3) which will issue a ticket that AAD will validate; AAD then issues an internal ticket. EXO reads this ticket and based on the username and groups within grants access to authorized mailboxes. No EXO customer content is sent outside of Office 365 other than to the customer and all customer interaction occurs over FIPS 140-2 compatible TLS (with the exception of customer-written emails sent to external email addresses). Customer content within EXO (i.e. email) is physically stored in Azure CONUS data centers and in Office 365 -specific racks for Office 365.

### SharePoint Online (SPO)

SharePoint Online (SPO) allows customers to share and manage content, knowledge, and applications to empower teamwork, quickly find information, and seamlessly collaborate across the organization.

SPO (including OneDrive for Business) is hosted on physical servers within Azure CONUS data centers. Network access to these servers is controlled by Azure-owned and managed network devices using rules managed by SPO and approved by Office 365 GCC High and DoD. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between SPO servers and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the data flow diagram and section 10.2 of this SSP, are allowed.

Microsoft administrators access SPO through remote desktop gateways managed by the Office 365 Remote Access Service (ORAS); this access requires multi-factor authentication.

Customer users interact with SPO through web browsers. The customer user authenticates to their own ADFS infrastructure which will issue a ticket that AAD will validate; AAD then issues an internal ticket. SPO reads the ticket and based on the username and groups within grants access to authorized SharePoint sites and files. No SPO customer content is sent outside of Office 365 GCC High and DoD other than to the customer, and customer interaction occurs over FIPS 140-2 compatible TLS 1.2. Customer content within SPO (i.e. SharePoint pages) is physically stored in Azure CONUS data centers and in Office 365 GCC High and DoD-specific racks for Office 365 GCC High and DoD.

Diagram

Description automatically generated

Figure 9‑5. SharePoint Online Data Flows

### Skype for Business (SFB)

Skype for Business (SFB) is a unified communications (UC) platform that integrates common channels of business communication and online meetings. It supports instant messaging, presence, audio and video calling, audio and video conferencing, and broadcast meetings. SFB integrates with Exchange and SharePoint.

SFB is hosted on physical servers within Azure data centers in CONUS, PaaS services on Azure, and uses Azure micro services such as Storage and Streaming Media.

The physical servers are joined to a security domain managed by SFB. Network access to these servers is controlled by Azure-managed network devices using rules managed by SFB and approved by Office 365 MT. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between SFB servers and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services, are allowed.

The Azure PaaS services are hosted on VMs managed by Azure (as PaaS) and physically reside in Azure CONUS datacenters. There is an ACL-based default-deny policy in place for all virtual machines that only allows use of explicitly defined ports/protocols necessary for delivery of the service. Only the flows documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services, are allowed. Azure services accessed by API only are managed as part of the Azure compliance portfolio.

Microsoft administrators access SFB through remote desktop gateways managed by ORAS; this access requires smartcard based multifactor authentication.

Users interact with SFB through the SFB client and web browsers. The user authenticates to their own ADFS infrastructure which will issue a ticket that AAD will validate; AAD then issues an internal ticket. SFB reads the ticket and based on the permissions grants access to authorized SFB sessions. Customer content is primarily handled internal to Office 365 services or on approved Azure services. All communications with the customer utilize FIPS 140-2 compatible TLS or SRTP protocols.

When stored, customer calls, messages, voicemail and IM conversations are stored within EXO. Content uploaded to a meeting is stored (encrypted) on SFB servers for the life of the meeting, and is deleted once the meeting ends. SFB physical servers reside in Azure CONUS data centers and in Office 365 GCC-specific racks for Office 365 GCC. Skype Broadcast Meetings can store encrypted meetings on Azure CDN. For GCC services, all Azure PAAS services consumed by SFB are hosted in the United States and are approved to handle data in accordance with the appropriate data handling standard.

SFB also offers public switched telephone network (PSTN) services like PSTN calling and PSTN conferencing. SFB PSTN services utilize existing SFB infrastructure and handle all data in accordance with Office 365 MT security controls. The Office 365 MT compliance boundary ends at the handoff of PSTN traffic to the PSTN provider. After the handoff PSTN traffic routes in accordance with telephony standards, and is outside the Office 365 MT compliance boundary.

Diagram

Description automatically generated

Figure 9‑5 Skype for Business Data Flows

### Office Online (WAC)

Office for the Web (internally known as WAC) provides customers the ability to view and edit, via web browser, documents in Office 365. Examples include EXO attachments, SFB / Teams presentations, and SPO documents. WAC also includes Office Collaboration Service (OCS) and Real Time Channel (RTC) both of which allow users to collaborate in real-time on SPO-hosted documents no matter which client the user is using (Desktop, Web, iPhone, Android).

WAC is hosted on Azure VMs and physically resides in Azure Government CONUS regions. Network access to these servers is controlled using Azure Network Security Groups managed by WAC and configured by Office 365 GCC High and DoD. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between WAC servers and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the data flow diagram below and Section 10.2 of this SSP, are allowed.

Microsoft administrators access WAC through remote desktop gateways managed by ORAS; this access requires multi-factor authentication.

Users interact with WAC; this interaction occurs via FIPS 140-2 compatible TLS 1.2. Documents viewed or edited in WAC are subject to the same access restrictions that are applied in EXO, SPO, or SFB. The user must first authenticate to EXO, SPO, or SFB which will then generate an access token which is sent to WAC. WAC passes that access token back to EXO, SPO, or SFB which validates it. Only valid tokens allow the user to view the requested content. No customer content is sent outside the system by WAC other than to the customer, and although WAC processes and temporarily caches customer content, WAC is a stateless service and does not permanently store any customer content.

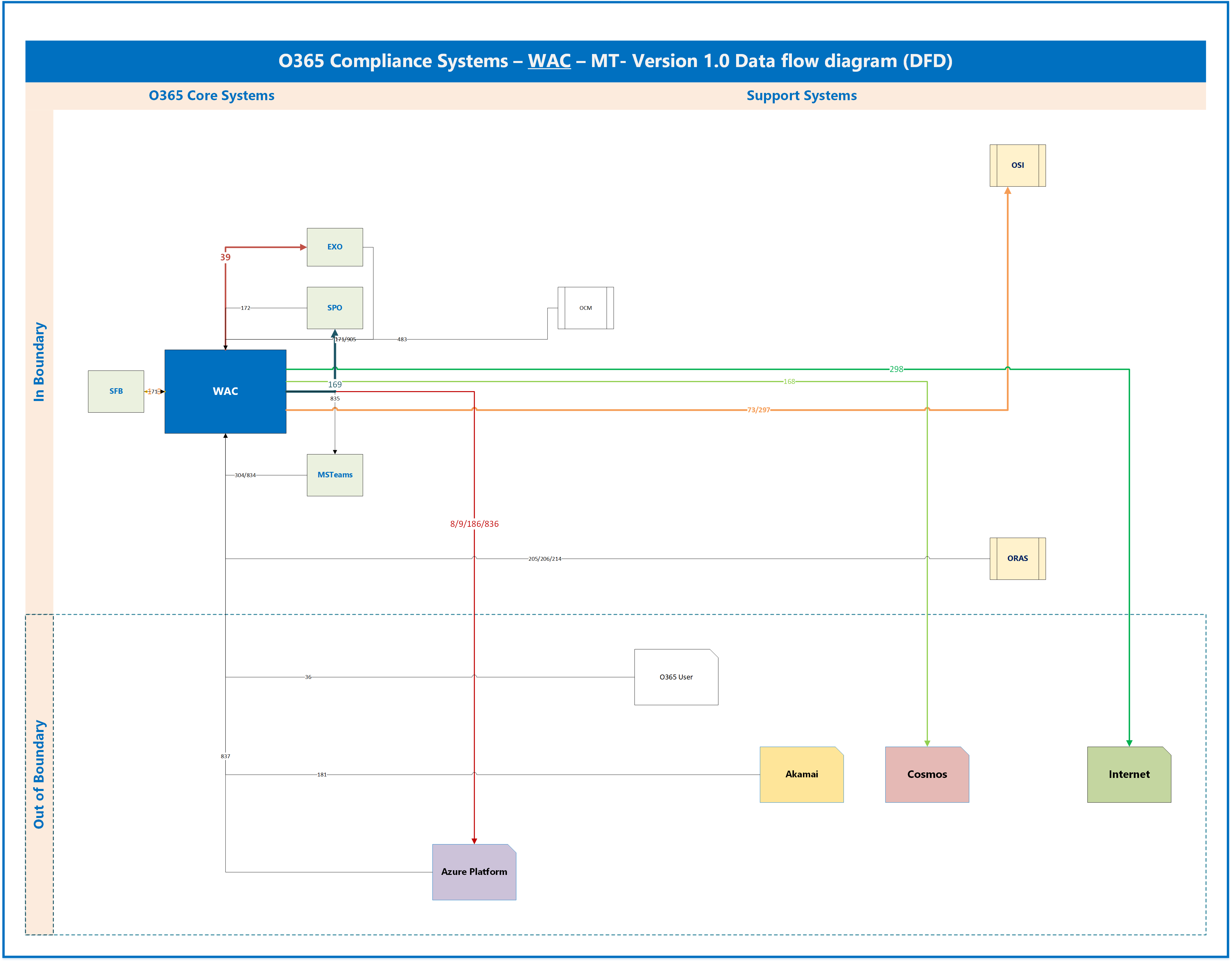


Figure 9‑6. Office Online Web Apps Data Flows

### Office 365 Remote Access Service (ORAS)

The Office 365 Remote Access Service (ORAS) provides a security domain and a set of remote Terminal Services Gateways (TSGs) used by service teams. The TSGs use Remote Desktop Protocol (RDP) over HTTPS to establish a secure, encrypted connection between remote users on the Internet and the internal network resources on which their productivity applications run.

ORAS is hosted on Azure virtual servers and physically resides in Azure CONUS datacenters. These servers are joined to a security domain managed by ORAS. Network access to these servers is controlled by Azure-managed network devices using rules managed by Azure and approved by Office 365. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between ORAS servers and other service teams, Microsoft networks, and the internet.

Microsoft administrators access ORAS through remote desktop gateways managed by ORAS; this access requires YubiKey-based multi-factor authentication.

Customer users and customer administrators do not interact with ORAS and ORAS does not process or store any customer content.

Graphical user interface

Description automatically generated with low confidence

Figure 9‑7. Office 365 Remote Access Service Data Flows

### Information Protection (IP)

Information Protection (IP, formerly named Exchange Online Protection (EOP)) provides anti-virus, anti-malware, and anti-spam filtering for email sent to Office 365 customers.

Data Loss Prevention (DLP) is a feature of Information Protection (IP). IP has built in message protections such as message hygiene, encryption, and other message protections in place to protect customer emails from unauthorized access and distribution.

IP is hosted on physical servers within Azure CONUS data centers and in Office 365-specific racks for Office 365. Network access to these servers is controlled by Azure-managed network devices using rules managed by IP and approved by Office 365. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between IP servers and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the data flow diagram and section 10.2 of this SSP, are allowed.

Microsoft administrators access ORAS through remote desktop gateways managed by the Office 365 Remote Access Service (ORAS); this access requires YubiKey-based multi-factor authentication.

If enabled by customer administrators, customer users can interact with IP via web browser to configure spam filter sensitivity and mail routing rules. The customer user authenticates to their own ADFS infrastructure which will issue a ticket that AAD will validate; AAD then issues an internal ticket. IP reads the ticket and based on the username and groups grants access to view and modify the appropriate mail rules. Customer emails are processed but not stored by IP. No IP customer content is sent outside of Office 365 other than to the customer and customer interaction occurs over FIPS 140-2 compatible TLS 1.2.

Diagram, schematic

Description automatically generated

Figure 9‑4. Information Protection Data Flows

### Office 365 Suite User Experience (SUE)

Suite User Experience (SUE) provides the web front end administrative interface for Microsoft 365 GCC High and DoD, including Teams, EXO, and SPO. SUE also provides a web GUI for users to configure settings delegated to them by customer administrators. SUE also includes service health monitoring functionality used by service team administrators to monitor their services.

SUE is hosted on virtual servers managed by Azure located in Azure Government CONUS data centers. Network access to these servers is controlled by Azure devices using rules managed by SUE and approved by Microsoft 365 GCC High and DoD. Azure is responsible for the implementation of network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between SUE virtual machines and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the data flow diagram below and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators do not access SUE virtual machines directly. They manage the service via the Azure Administrative Portal run by Azure. This access requires multi-factor authentication.

Users interact with SUE when accessing SFB, EXO, and SPO administration portals via web browser; these interactions are protected by FIPS 140-2 compatible TLS 1.2. SUE is a stateless service and does not store any customer content.

Diagram

Description automatically generated

Figure 9‑8. Suite User Experience Data Flows

### Office Service Infrastructure (OSI)

Office Service Infrastructure (OSI) provides a platform for backend applications that enhance the overall Office 365 service offering. OSI is hosted on Azure and contains deployment, hosting and monitoring infrastructure applications which include services as Forms, Planner, Click2Run, Office Licensing Service, and Roaming, etc.

OSI and the applications hosted on OSI are hosted on virtual servers managed by Azure, and Azure is responsible for ensuring that OSI virtual machines are provisioned in Azure CONUS data centers. Network access to these servers is controlled by Azure devices using rules managed by OSI and approved by Office 365. Azure provides the implementation of network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between SUE virtual machines and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators access OSI provisioned virtual machines via RDP. This process requires enabling an account with a random password and then connecting using that account. This process is gated by two-factor authentication. Users do not interact with OSI and OSI does not store customer content. Connections between Office applications or SUE and OSI occur over FIPS 140-2 compatible TLS 1.2.

Graphical user interface

Description automatically generated with low confidence

Figure 9‑9. Office Service Infrastructure Data Flows

### 9.5.9. Azure Active Directory (AAD)

Azure Active Directory (AAD) supports customer authentication but is not part of the Office 365 accreditation boundary. Azure Active Directory provides a single-sign-on identity and access management solution along with a robust set of tools to manage users and groups. This solution provides secure access to the Office 365 online services. Full details of AAD’s security architecture and control implementations can be found in the Microsoft Azure SSP. AAD contains backend services which provide user account management, including the services that support ADFS as described in section 9.1.2.

Customers are required to enable Active Directory Federation Services (ADFS) to manage their users’ identities and authorizations. Users do not interact with AAD directly. Connections between AAD and the customer’s Active Directory infrastructure are protected via FIPS-validated TLS 1.2.

Diagram

Description automatically generated

Figure 9‑10. Azure Active Directory Data Flows

### 9.5.10. Microsoft Teams (MSTeams)

Microsoft Teams (MSTeams) is an immersive workspace solution that provides instant messaging and group chat, voice/video calling and conferencing, file sharing, and shared workspace. Microsoft administrators access MSTeams through remote desktop gateways managed by ORAS; this access requires YubiKey-based multi-factor authentication.

MSTeams is hosted on physical servers within Azure CONUS data centers managed by Azure and use the Azure Pilotfish service, as well as Azure micro services such as Storage and Streaming Media. The physical servers may be joined to a security domain managed by Azure. Network access to these servers is controlled by Azure-managed network devices using rules managed by Skype organization and approved by Office 365. Azure also implements network intrusion detection and denial of service protection. All Azure based services are hosted on VMs, or hardware managed by Azure. There is an ACL-based default-deny policy in place for all virtual machines that only allows use of explicitly defined ports/protocols necessary for delivery of the service. Only the flows documented in the above data flow diagram and section 9.5 of this SSP, are allowed. Azure services accessed by API only are managed as part of the Azure compliance portfolio.

Users interact with MSTeams through the MSTeams client and web browsers. The user authenticates to their own ADFS infrastructure which will issue a ticket that AAD will validate; AAD and MSTeams then issue internals tickets to be used to access various components. MSTeams reads the ticket and based on the permissions grants access to authorized MSTeams resources. Customer content is primarily handled internal to O365 services or on approved Azure services. All communications with the customer utilize FIPS 140-2 compatible protocols. When stored, customer calls, messages, voicemail and IM conversations are stored in EXO, Azure storage, or Object Store. Content uploaded to MSTeams is stored in SharePoint. For GCC services, all Azure PaaS services consumed by MSTeams are hosted in the United States and are approved to handle data in accordance with the appropriate data handling standard.

Diagram, timeline

Description automatically generated

Figure 9‑12. Microsoft Teams Data Flows

### 9.5.11. Bing

The Bing service consists of several first party, backend services (Falcon, Object Store, QAS) designed to support customer facing Office 365 services.

Connections with Bing teams occur over FIPS 140-2 validated TLS 1.2. Additionally, customer content stored by Bing teams are encrypted with a FIPS 140-2 validated algorithm. Users do not directly interact with customer content stored by Bing.

Some Bing teams are hosted on servers managed by Pilotfish within Azure CONUS data centers. This includes the management of baseline configurations and hardware components. Additionally, Pilotfish provides antivirus scanning as well as BeyondTrust vulnerability scanning. There is an ACL-based default-deny policy in place between Bing servers and other service teams, Microsoft networks, and the internet.

K9 is the security monitoring capability is provided through Pilotfish. K9 is used by some teams to collect, store and perform real-time analysis on security logs to flag suspected intrusions or unusual activity. Bing teams coordinate with both Pilotfish and the Office 365 Security and Incident Response teams on events requiring further investigation.

Microsoft administrators access Bing teams through remote desktop gateways managed by ORAS; this access requires YubiKey-based multi-factor authentication.

A picture containing box and whisker chart

Description automatically generated

Figure 9‑11. Bing Data Flows

### 9.5.12. Activity Feed Service (AFS)

The Activity Feed Service (AFS) is a high scale, low latency data roaming service. AFS enables the collection and synchronization of a customer’s data across devices and applications connected to his AAD or Microsoft account, powering features such as Windows Timeline, Cloud Clipboard & Windows Settings Sync.

AFS is hosted on servers managed by PilotFish within Azure CONUS data centers. This includes the management of baseline configurations and hardware components as well as antivirus scanning. There is a default-deny network access policy in place between AFS virtual machines and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the data flow diagram below and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators do not access AFS hosts directly. Administrators access the service through remote desktop gateways managed by the Torus Remote Access Service; this access requires multifactor authentication.

Customers do not interact directly with AFS. Applications publish data to AFS on the customer’s behalf. Connections to AFS occur over FIPS 140-2 validated TLS. Customer data which is persisted for longer than 24 hours is stored in Exchange.

Diagram

Description automatically generated

Figure 9‑13. Activity Feed Service Data Flows

### 9.5.13. Search Content Service (SCS)

The Search Content Service (SCS) is a backend service that enables SharePoint document search. SCS receives a real-time stream of parsed changes to documents (create, update, delete) from SharePoint Online (SPO) or a customer’s on-premise SharePoint instance. This data is then pushed to search indexes. Customers do not interact directly with SCS.

SCS is hosted on Azure virtual servers within Azure CONUS data centers. Network access to these servers is controlled by Azure devices using rules managed by SCS and approved by Office 365. Azure is responsible for the implementation of network intrusion detection and denial of service protection. Microsoft administrators do not access SCS virtual machines directly. Authorized administrators access the SCS environment through gateways which requires multifactor authentication. Network access to these servers is controlled by Azure-managed network devices and approved by Office 365.

Connections with SCS occur over FIPS 140-2 validated TLS. Customer content collected by SCS is stored encrypted in Azure storage.

Diagram

Description automatically generated

Figure 9‑14. Search Content Service Data Flows

### 9.5.14. Office Intelligent Services (IS)

Office Intelligent Services back features in the Windows, Mac, iOS, Android, and online clients. These features and services enhance the user's experience with Office and allow them to achieve more.

Features include: Augmentation Loop, Enrichment, Image-To-Doc, Editor, Grammar, Translation, Scripts, Templates, Dictation, PowerPoint Presentation Coach, Transcription, PowerPoint Designer, Recent Documents, Smart Lookup, Tell Me, and Word/Excel/PowerPoint Conversion Services

Licensing, Device Management, Configuration, Sign-in, Redirection, Roaming settings are also considered part of this bucket.

Office Intelligent Services is also responsible for full online services from Forms, Planner, Sway, Desktop Admin Portal, Fluid, and Whiteboard.

Diagram

Description automatically generated

Figure 9‑15. Office Intelligent Services Data Flows

### 9.5.15. Customer Insight and Analysis (CIA)

Customer Insight and Analysis (CIA), also known as “Usage Reports," is a reporting service in the tenant Admin Portal to show data such as O365 license consumption and service usage to assist with making business decisions.

CIA is hosted on Azure virtual servers within Azure CONUS data centers. Network access to these servers is controlled by Azure devices using rules managed by CIA and approved by Office 365. Microsoft administrators do not access CIA virtual machines directly. Administrators access the CIA environment through gateways which requires multifactor authentication. Network access to these servers is controlled by Azure-managed network devices and approved by Office 365. Azure also implements network intrusion detection and denial of service protection.

Customers interact with CIA via the Customer Admin Portal. Connections with CIA occur over FIPS 140-2 validated TLS. Customer content collected by CIA is stored and encrypted in Azure storage.

Diagram, box and whisker chart

Description automatically generated

Figure 9‑16. Customer Insight and Analysis Data FlowsCloud Input Intelligence (CII)



### Cloud Input Intelligence (CII)

Diagram

Description automatically generated

Figure 9‑19 Cloud Input Intelligence Data Flows

Cloud Input Intelligence (CII), also known as “Windows Ink,” provides a compliant platform that allows developers to provide cutting-edge capabilities on all devices, utilizing data driven personalized experiences that capture user intent on technology that will be always-learning more over time. This service enables applications built on the CII service to provide improved experiences in inking, text entry and other input modalities across a user's devices.

CII is driven by a set of Service Fabric applications hosted within Azure CONUS data centers and managed by CII utilizing the rules established by the Office 365 Trust team. CII uses Azure API Management (APIM) to act as the front door service for the REST APIs exposed to the application developers. APIM has the capability to throttle incoming traffic and apply policy rules which are implemented by the CII team to provide denial of service protection. APIM also is constrained to use TLS 1.2 and HTTPS for all communications with the calling application. In addition, all clusters have a highly restrictive set of network routing rules to prevent access to most ports and utilizes a certificate-based handshake between all callers (exclusively APIM) and the clusters to prevent unauthorized access over the ports that are open. ​

All subscriptions are owned by the Torus tenant and authorized On-Call engineers must elevate using a smart card and email approval process which provides access to the environment via Azure Portal. Just In Time access to Azure VMs utilizes a similar mechanism and real time created accounts with unique passwords which expire after a given time period.

CII is a stateless service and does not store any customer content. Callers to the service are exclusively applications that have been authorized access to the APIM instance via a subscription key. Calls without a valid subscription key are rejected by API Management.​

### Live People Card

Live People Card, also known as “Loki,” is an Azure hosted service which powers people experiences with low latency across different O365 products (for example: Outlook, SharePoint, OneDrive). Example people experiences powered by Loki are Live Persona Cards and People Hub. It is a stateless service that doesn’t master data. The data served back to Loki’s clients is coming from Loki’s dependency services (for example Exchange, Microsoft Graph, SPO). For better performance, Loki is using Redis to cache encrypted customer data for up to 24 hours.

Loki is hosted on Azure virtual servers within Azure CONUS data centers. Network access to these servers is controlled by Azure devices using rules managed by Loki and approved by Office 365. Azure is responsible for implementation of network intrusion detection and denial of service protection. There is a default-deny network access policy in place between Loki virtual machines and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators do not access Loki virtual machines directly. Administrators access the service through a “jump box” VM in the Loki environment and remote desktop gateways managed by ORAS; this access requires YubiKey-based multifactor authentication.

Customers interact with Loki via web browser protected by FIPS 140-2 compatible TLS.

Graphical user interface

Description automatically generated with medium confidence

Figure 9‑17. Loki Data Flows

### Delve

Diagram, box and whisker chart

Description automatically generated

Figure 9‑16 Delve Data Flows

Delve allows customers to manage their Office 365 profile, and to discover and organize the information that's likely to be most interesting across Office 365. Delve determines the relevancy of information based on the user's relationships as well as activity within the user’s organization.

Delve is hosted on virtual servers managed by Azure within Azure CONUS datacenters. Network access to these servers is controlled by Azure devices using rules managed by Delve and approved by Office 365 MT. Azure is responsible for implementation of network intrusion detection and denial of service protection. There is a default-deny network access policy in place between Delve virtual machines and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators do not access Delve virtual machines directly. Administrators access the service through a “jump box” VM in the Delve environment and remote desktop gateways managed by ORAS; this access requires YubiKey-based multifactor authentication.

Customers interact with Delve via web browser protected by FIPS 140-2 compatible TLS.

# System Environment and Inventory

Directions for attaching the FedRAMP Inventory Workbook may be found in the following section: Attachment 13, FedRAMP Inventory Workbook.

## Data Flow

The data flow in and out of the system boundaries is represented in Figure 10-1. Data Flow Diagram, below.



Figure 10‑1. Data Flow Diagram

The above diagram and accompanying legend documents all data flows between Office 365 service teams, between Office 365 and interconnected systems, and between Office 365 and customers. The data flows involving customer content are discussed here in narrative format, but detailed information about each flow, including source and destination, is available from Microsoft, provided appropriate confidentiality agreements are in place.

## 10.2. Ports, Protocols and Services

Due to the scale of the Microsoft Office 365 environment, the Ports, Protocols, and Services table is provided in Attachment 14 – Ports & Protocols.

# System Interconnections

Table 11‑1 System Interconnections below is consistent with Table 13‑3 CA-3 Authorized Connections.

Table 11‑1. System Interconnections

| SP\* IP Address and Interface | External Organization Name and IP Address of System | External Point of Contact and Phone Number | Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)\*\* | Data Direction  (incoming, outgoing, or both) | Information Being Transmitted | Port or Circuit Numbers |
| --- | --- | --- | --- | --- | --- | --- |
| N/A | Core Services Engineering (CSE, formerly MSIT) CorpNet | Lisa Reshaur  (425) 703-1935 | TLS | Both | System Documentation, build information, change ticketing | N/A |
| N/A | Azure | Tom Keane  425-241-1298 | TLS | Both | System data | N/A |
| N/A | Cosmos | Ryan Waite  (425) 706-1894 | TLS | Both | Scrubbed log data | N/A |
| N/A | Office 365 Support | Elisabeth Zornes  (415) 229-0349 | TLS | Both | Basic account information | N/A |
| N/A | Universal Store | Doug Taylor  (425) 707-4908 | TLS | Both | Commercial Customer Billing Information | N/A |
| N/A | Akamai | David Yoon  (703) 621-4023 | TLS | Both | static website content | N/A |

\*Service Processor

\*\*Internet Protocol Security (IPSec), Virtual Private Network (VPN), Secure Sockets Layer (SSL)

# Laws, Regulations, Standards and Guidance

A summary of FedRAMP Laws and Regulations is included in ATTACHMENT 12 – FedRAMP Laws and Regulations.

## Applicable Laws and Regulations

The FedRAMP Laws and Regulations can be found on this web page: [Templates.](https://www.fedramp.gov/templates)

Table 12-1 Office 365 Law and Regulations includes additional laws and regulations specific to Office 365.

Table 12‑1. Office 365 Laws and Regulations

| **Identification Number** | **Title** | **Date** | **Link** |
| --- | --- | --- | --- |
|  | N/A |  |  |

## Applicable Standards and Guidance

The FedRAMP Standards and Guidance be found on this web page: [Templates](https://www.fedramp.gov/templates)

Table 12‑2 Office 365 MT Standards and Guidance includes in this section any additional standards and guidance specific to Office 365.

Table 12‑2. Office 365 MT Standards and Guidance

| **Identification Number** | **Title** | | | **Date** | **Link** |
| --- | --- | --- | --- | --- | --- |
|  | | Department of Defense Cloud Computing Security Requirements Guide V1 R3 | 12/18/17 | | [DISA SRG 1.3](https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf) |

# Minimum Security Controls

Security controls must meet minimum security control baseline requirements. Upon categorizing a system as Low, Moderate, or High sensitivity in accordance with FIPS 199, the corresponding security control baseline standards apply. Some of the control baselines have enhanced controls which are indicated in parentheses.

Security controls that are representative of the sensitivity of Office 365 are described in the sections that follow. Security controls that are designated as “Not Selected” or “Withdrawn by NIST” are not described unless they have additional FedRAMP controls. Guidance on how to describe the implemented standard can be found in NIST 800-53, Rev 4. Control enhancements are marked in parentheses in the sensitivity columns.

Systems that are categorized as FIPS 199 Low use the controls designated as Low, systems categorized as FIPS 199 Moderate use the controls designated as Moderate and systems categorized as FIPS 199 High use the controls designated as High. A summary of which security standards pertain to which sensitivity level is found in Table 13‑1 Summary of Required Security Controls that follows.

*Table 13‑1. Summary of Required Security Controls*

| *ID* | *Control Description* | *Sensitivity Level* | | | |
| --- | --- | --- | --- | --- | --- |
| *Low* | *Moderate* | *High* | |
| AC | Access Control | | | | |
| AC-1 | Access Control Policy and Procedures | AC-1 | AC-1 | AC-1 | |
| AC-2 | Account Management | AC-2 | AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12) | AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (11) (12) (13) | |
| AC-3 | Access Enforcement | AC-3 | AC-3 | AC-3 | |
| AC-4 | Information Flow Enforcement | Not Selected | AC-4 (21) | AC-4 (8) (21) | |
| AC-5 | Separation of Duties | Not Selected | AC-5 | AC-5 | |
| AC-6 | Least Privilege | Not Selected | AC-6 (1) (2) (5) (9) (10) | AC-6 (1) (2) (3) (5) (7) (8) (9) (10) | |
| AC-7 | Unsuccessful Logon Attempts | AC-7 | AC-7 | AC-7 (2) | |
| AC-8 | System Use Notification | AC-8 | AC-8 | AC-8 | |
| AC-10 | Concurrent Session Control | Not Selected | AC-10 | AC-10 | |
| AC-11 | Session Lock | Not Selected | AC-11 (1) | AC-11 (1) | |
| AC-12 | Session Termination | Not Selected | AC-12 | AC-12 (1) | |
| AC-14 | Permitted Actions Without Identification or Authentication | AC-14 | AC-14 | AC-14 | |
| AC-17 | Remote Access | AC-17 | AC-17 (1) (2) (3) (4) (9) | AC-17 (1) (2) (3) (4) (9) | |
| AC-18 | Wireless Access | AC-18 | AC-18 (1) | AC-18 (1) (3) (4) (5) | |
| AC-19 | Access Control For Mobile Devices | AC-19 | AC-19 (5) | AC-19 (5) | |
| AC-20 | Use of External Information Systems | AC-20 | AC-20 (1) (2) | AC-20 (1) (2) | |
| AC-21 | Information Sharing | Not Selected | AC-21 | AC-21 | |
| AC-22 | Publicly Accessible Content | AC-22 | AC-22 | AC-22 | |
| AC-23 | Data Mining Protection | Not Selected | Not Selected | Not Selected | |
| AT | Awareness and Training | | | | |
| AT-1 | Security Awareness and Training Policy and Procedures | AT-1 | AT-1 | AT-1 | |
| AT-2 | Security Awareness Training | AT-2 | AT-2 (2) | AT-2 (2) | |
| AT-3 | Role-Based Security Training | AT-3 | AT-3 | AT-3 (3) (4) | |
| AT-4 | Security Training Records | AT-4 | AT-4 | AT-4 | |
| AU | Audit and Accountability | | | | |
| AU-1 | Audit and Accountability Policy and Procedures | AU-1 | AU-1 | AU-1 | |
| AU-2 | Audit Events | AU-2 | AU-2 (3) | AU-2 (3) | |
| AU-3 | Content of Audit Records | AU-3 | AU-3 (1) | AU-3 (1) (2) | |
| AU-4 | Audit Storage Capacity | AU-4 | AU-4 | AU-4 | |
| AU-5 | Response to Audit Processing Failures | AU-5 | AU-5 | AU-5 (1) (2) | |
| AU-6 | Audit Review, Analysis and Reporting | AU-6 | AU-6 (1) (3) | AU-6 (1) (3) (4) (5) (6) (7) (10) | |
| AU-7 | Audit Reduction and Report Generation | Not Selected | AU-7 (1) | AU-7 (1) | |
| AU-8 | Time Stamps | AU-8 | AU-8 (1) | AU-8 (1) | |
| AU-9 | Protection of Audit Information | AU-9 | AU-9 (2) (4) | AU-9 (2) (3) (4) | |
| AU-10 | Non-repudiation | Not Selected | Not Selected | AU-10 | |
| AU-11 | Audit Record Retention | AU-11 | AU-11 | AU-11 | |
| AU-12 | Audit Generation | AU-12 | AU-12 | AU-12 (1) (3) | |
| AU-16 | Sharing of Audit Information |  |  |  | |
| CA | Security Assessment and Authorization | | | | |
| CA-1 | Security Assessment and Authorization Policies and Procedures | CA-1 | CA-1 | CA-1 | |
| CA-2 | Security Assessments | CA-2 (1) | CA-2 (1) (2) (3) | CA-2 (1) (2) (3) | |
| CA-3 | System Interconnections | CA-3 | CA-3 (3) (5) | CA-3 (3) (5) | |
| CA-5 | Plan of Action and Milestones | CA-5 | CA-5 | CA-5 | |
| CA-6 | Security Authorization | CA-6 | CA-6 | CA-6 | |
| CA-7 | Continuous Monitoring | CA-7 | CA-7 (1) | CA-7 (1) (3) | |
| CA-8 | Penetration Testing | Not Selected | CA-8 (1) | CA-8 (1) | |
| CA-9 | Internal System Connections | CA-9 | CA-9 | CA-9 | |
| CM | Configuration Management | | | | |
| CM-1 | Configuration Management Policy and Procedures | CM-1 | CM-1 | CM-1 | |
| CM-2 | Baseline Configuration | CM-2 | CM-2 (1) (2) (3) (7) | CM-2 (1) (2) (3) (7) | |
| CM-3 | Configuration Change Control | Not Selected | CM-3 (2) | CM-3 (1) (2) (4) (6) | |
| CM-4 | Security Impact Analysis | CM-4 | CM-4 | CM-4 (1) | |
| CM-5 | Access Restrictions For Change | Not Selected | CM-5 (1) (3) (5) | CM-5 (1) (2) (3) (5) | |
| CM-6 | Configuration Settings | CM-6 | CM-6 (1) | CM-6 (1) (2) | |
| CM-7 | Least Functionality | CM-7 | CM-7 (1) (2) (5)\* | CM-7 (1) (2) (5) | |
| CM-8 | Information System Component Inventory | CM-8 | CM-8 (1) (3) (5) | CM-8 (1) (2) (3) (4) (5) | |
| CM-9 | Configuration Management Plan | Not Selected | CM-9 | CM-9 | |
| CM-10 | Software Usage Restrictions | CM-10 | CM-10 (1) | CM-10 (1) | |
| CM-11 | User-Installed Software | CM-11 | CM-11 | CM-11 (1) | |
| \*FedRAMP does not include CM-7 (4) in the Moderate Baseline. NIST supplemental guidance states that CM-7 (4) is not required if (5) is implemented. | | | | |
| CP | Contingency Planning | | | | |
| CP-1 | Contingency Planning Policy and Procedures | CP-1 | CP-1 | CP-1 | |
| CP-2 | Contingency Plan | CP-2 | CP-2 (1) (2) (3) (8) | CP-2 (1) (2) (3) (4) (5) (8) | |
| CP-3 | Contingency Training | CP-3 | CP-3 | CP-3 (1) | |
| CP-4 | Contingency Plan Testing | CP-4 | CP-4 (1) | CP-4 (1) (2) | |
| CP-6 | Alternate Storage Site | Not Selected | CP-6 (1) (3) | CP-6 (1) (2) (3) | |
| CP-7 | Alternate Processing Site | Not Selected | CP-7 (1) (2) (3) | CP-7 (1) (2) (3) (4) | |
| CP-8 | Telecommunications Services | Not Selected | CP-8 (1) (2) | CP-8 (1) (2) (3) (4) | |
| CP-9 | Information System Backup | CP-9 | CP-9 (1) (3) | CP-9 (1) (2) (3) (5) | |
| CP-10 | Information System Recovery and Reconstitution | CP-10 | CP-10 (2) | CP-10 (2) (4) | |
|  |  |  |  |  | |
| IA | Identification and Authentication | | | | |
| IA-1 | Identification and Authentication Policy and Procedures | IA-1 | IA-1 | IA-1 | |
| IA-2 | Identification and Authentication (Organizational Users) | IA-2 (1) (12) | IA-2 (1) (2) (3) (5) (8) (11) (12) | IA-2 (1) (2) (3) (4) (5) (8) (9) (11) (12) | |
| IA-3 | Device Identification and Authentication | Not Selected | IA-3 | IA-3 | |
| IA-4 | Identifier Management | IA-4 | IA-4 (4) | IA-4 (4) | |
| IA-5 | Authenticator Management | IA-5 (1) (11) | IA-5 (1) (2) (3) (4) (6) (7) (11) | IA-5 (1) (2) (3) (4) (6) (7) (8) (11) (13) | |
| IA-6 | Authenticator Feedback | IA-6 | IA-6 | IA-6 | |
| IA-7 | Cryptographic Module Authentication | IA-7 | IA-7 | IA-7 | |
| IA-8 | Identification and Authentication (Non-Organizational Users) | IA-8 (1) (2) (3) (4) | IA-8 (1) (2) (3) (4) | IA-8 (1) (2) (3) (4) | |
|  |  |  |  |  | |
| AT | Awareness and Training | | | | |
| IR-1 | Incident Response Policy and Procedures | IR-1 | IR-1 | IR-1 | |
| IR-2 | Incident Response Training | IR-2 | IR-2 | IR-2 (1) (2) | |
| IR-3 | Incident Response Testing | Not Selected | IR-3 (2) | IR-3 (2) | |
| IR-4 | Incident Handling | IR-4 | IR-4 (1) | IR-4 (1) (2) (3) (4) (6) (8) | |
| IR-5 | Incident Monitoring | IR-5 | IR-5 | IR-5 (1) | |
| IR-6 | Incident Reporting | IR-6 | IR-6 (1) | IR-6 (1) | |
| IR-7 | Incident Response Assistance | IR-7 | IR-7 (1) (2) | IR-7 (1) (2) | |
| IR-8 | Incident Response Plan | IR-8 | IR-8 | IR-8 | |
| IR-9 | Information Spillage Response | Not Selected | IR-9 (1) (2) (3) (4) | IR-9 (1) (2) (3) (4) | |
|  |  |  |  |  | |
| MA | Maintenance | | | | |
| MA-1 | System Maintenance Policy and Procedures | MA-1 | MA-1 | MA-1 | |
| MA-2 | Controlled Maintenance | MA-2 | MA-2 | MA-2 (2) | |
| MA-3 | Maintenance Tools | Not Selected | MA-3 (1) (2) (3) | MA-3 (1) (2) (3) | |
| MA-4 | Nonlocal Maintenance | MA-4 | MA-4 (2) | MA-4 (2) (3) (6) | |
| MA-5 | Maintenance Personnel | MA-5 | MA-5 (1) | MA-5 (1) | |
| MA-6 | Timely Maintenance | Not Selected | MA-6 | MA-6 | |
| MP | Media Protection | | | | |
| MP-1 | Media Protection Policy and Procedures | MP-1 | MP-1 | MP-1 | |
| MP-2 | Media Access | MP-2 | MP-2 | MP-2 | |
| MP-3 | Media Marking | Not Selected | MP-3 | MP-3 | |
| MP-4 | Media Storage | Not Selected | MP-4 | MP-4 | |
| MP-5 | Media Transport | Not Selected | MP-5 (4) | MP-5 (4) | |
| MP-6 | Media Sanitization | MP-6 | MP-6 (2) | MP-6 (1) (2) (3) | |
| MP-7 | Media Use | MP-7 | MP-7 (1) | MP-7 (1) | |
|  |  |  |  |  | |
| PE | Physical and Environmental Protection | | | | |
| PE-1 | Physical and Environmental Protection Policy and Procedures | PE-1 | PE-1 | PE-1 | |
| PE-2 | Physical Access Authorizations | PE-2 | PE-2 | PE-2 | |
| PE-3 | Physical Access Control | PE-3 | PE-3 | PE-3 (1) | |
| PE-4 | Access Control For Transmission Medium | Not Selected | PE-4 | PE-4 | |
| PE-5 | Access Control For Output Devices | Not Selected | PE-5 | PE-5 | |
| PE-6 | Monitoring Physical Access | PE-6 | PE-6 (1) | PE-6 (1) (4) | |
| PE-8 | Visitor Access Records | PE-8 | PE-8 | PE-8 (1) | |
| PE-9 | Power Equipment and Cabling | Not Selected | PE-9 | PE-9 | |
| PE-10 | Emergency Shutoff | Not Selected | PE-10 | PE-10 | |
| PE-11 | Emergency Power | Not Selected | PE-11 | PE-11 (1) | |
| PE-12 | Emergency Lighting | PE-12 | PE-12 | PE-12 | |
| PE-13 | Fire Protection | PE-13 | PE-13 (2) (3) | PE-13 (1) (2) (3) | |
| PE-14 | Temperature and Humidity Controls | PE-14 | PE-14 (2) | PE-14 (2) | |
| PE-15 | Water Damage Protection | PE-15 | PE-15 | PE-15 (1) | |
| PE-16 | Delivery and Removal | PE-16 | PE-16 | PE-16 | |
| PE-17 | Alternate Work Site | Not Selected | PE-17 | PE-17 | |
| PE-18 | Location of Information System Components | Not Selected | Not Selected | PE-18 | |
| PL | Planning | | | | |
| PL-1 | Security Planning Policy and Procedures | PL-1 | PL-1 | PL-1 | |
| PL-2 | System Security Plan | PL-2 | PL-2 (3) | PL-2 (3) | |
| PL-4 | Rules of Behavior | PL-4 | PL-4 (1) | PL-4 (1) | |
| PL-8 | Information Security Architecture | Not Selected | PL-8 | PL-8 | |
|  |  |  |  |  | |
| PS | Personnel Security | | | | |
| PS-1 | Personnel Security Policy and Procedures | PS-1 | PS-1 | PS-1 | |
| PS-2 | Position Risk Designation | PS-2 | PS-2 | PS-2 | |
| PS-3 | Personnel Screening | PS-3 | PS-3 (3) | PS-3 (3) | |
| PS-4 | Personnel Termination | PS-4 | PS-4 | PS-4 (2) | |
| PS-5 | Personnel Transfer | PS-5 | PS-5 | PS-5 | |
| PS-6 | Access Agreements | PS-6 | PS-6 | PS-6 | |
| PS-7 | Third-Party Personnel Security | PS-7 | PS-7 | PS-7 | |
| PS-8 | Personnel Sanctions | PS-8 | PS-8 | PS-8 | |
| RA | Risk Assessment | | | | |
| RA-1 | Risk Assessment Policy and Procedures | RA-1 | RA-1 | RA-1 | |
| RA-2 | Security Categorization | RA-2 | RA-2 | RA-2 | |
| RA-3 | Risk Assessment | RA-3 | RA-3 | RA-3 | |
| RA-5 | Vulnerability Scanning | RA-5 | RA-5 (1) (2) (3) (5) (6) (8) | RA-5 (1) (2) (3) (4) (5) (6) (8) (10) | |
| SA | System and Services Acquisition | | | | |
| SA-1 | System and Services Acquisition Policy and Procedures | SA-1 | SA-1 | SA-1 | |
| SA-2 | Allocation of Resources | SA-2 | SA-2 | SA-2 | |
| SA-3 | System Development Life Cycle | SA-3 | SA-3 | SA-3 | |
| SA-4 | Acquisition Process | SA-4 (10) | SA-4 (1) (2) (8) (9) (10) | SA-4 (1) (2) (8) (9) (10) | |
| SA-5 | Information System Documentation | SA-5 | SA-5 | SA-5 | |
| SA-8 | Security Engineering Principles | Not Selected | SA-8 | SA-8 | |
| SA-9 | External Information System Services | SA-9 | SA-9 (1) (2) (4) (5) | SA-9 (1) (2) (4) (5) | |
| SA-10 | Developer Configuration Management | Not Selected | SA-10 (1) | SA-10 (1) | |
| SA-11 | Developer Security Testing and Evaluation | Not Selected | SA-11 (1) (2) (8) | SA-11 (1) (2) (8) | |
| SA-12 | Supply Chain Protection | Not Selected | Not Selected | SA-12 | |
| SA-15 | Development Process, Standards and Tools | Not Selected | Not Selected | SA-15 | |
| SA-16 | Developer-Provided Training | Not Selected | Not Selected | SA-16 | |
| SA-17 | Developer Security Architecture and Design | Not Selected | Not Selected | SA-17 | |
|  |  |  |  |  | |
| SC | System and Communications Protection | | | | |
| SC-1 | System and Communications Protection Policy and Procedures | SC-1 | SC-1 | SC-1 | |
| SC-2 | Application Partitioning | Not Selected | SC-2 | SC-2 | |
| SC-3 | Security Function Isolation | Not Selected | Not Selected | SC-3 | |
| SC-4 | Information In Shared Resources | Not Selected | SC-4 | SC-4 | |
| SC-5 | Denial of Service Protection | SC-5 | SC-5 | SC-5 | |
| SC-6 | Resource Availability | Not Selected | SC-6 | SC-6 | |
| SC-7 | Boundary Protection | SC-7 | SC-7 (3) (4) (5) (7) (8) (12) (13) (18) | SC-7 (3) (4) (5) (7) (8) (10) (12) (13) (18) (20) (21) | |
| SC-8 | Transmission Confidentiality and Integrity | Not Selected | SC-8 (1) | SC-8 (1) | |
| SC-10 | Network Disconnect | Not Selected | SC-10 | SC-10 | |
| SC-12 | Cryptographic Key Establishment and Management | SC-12 | SC-12 (2) (3) | SC-12 (1) (2) (3) | |
| SC-13 | Cryptographic Protection | SC-13 | SC-13 | SC-13 | |
| SC-15 | Collaborative Computing Devices | SC-15 | SC-15 | SC-15 | |
| SC-17 | Public Key Infrastructure Certificates | Not Selected | SC-17 | SC-17 | |
| SC-18 | Mobile Code | Not Selected | SC-18 | SC-18 | |
| SC-19 | Voice Over Internet Protocol | Not Selected | SC-19 | SC-19 | |
| SC-20 | Secure Name / Address Resolution Service (Authoritative Source) | SC-20 | SC-20 | SC-20 | |
| SC-21 | Secure Name / Address Resolution Service (Recursive or Caching Resolver) | SC-21 | SC-21 | SC-21 | |
| SC-22 | Architecture and Provisioning for Name / Address Resolution Service | SC-22 | SC-22 | SC-22 | |
| SC-23 | Session Authenticity | Not Selected | SC-23 | SC-23 (1) | |
| SC-24 | Fail in Known State | Not Selected | Not Selected | SC-24 | |
| SC-28 | Protection of Information At Rest | Not Selected | SC-28 (1) | SC-28 (1) | |
| SC-39 | Process Isolation | SC-39 | SC-39 | SC-39 | |
|  |  |  |  |  | |
| SI | System and Information Integrity | | | | |
| SI-1 | System and Information Integrity Policy and Procedures | SI-1 | SI-1 | SI-1 | |
| SI-2 | Flaw Remediation | SI-2 | SI-2 (2) (3) | SI-2 (1) (2) (3) | |
| SI-3 | Malicious Code Protection | SI-3 | SI-3 (1) (2) (7) | SI-3 (1) (2) (7) | |
| SI-4 | Information System Monitoring | SI-4 | SI-4 (1) (2) (4) (5) (14) (16) (23) | SI-4 (1) (2) (4) (5) (11) (14) (16) (18) (19) (20) (22) (23) (24) | |
| SI-5 | Security Alerts, Advisories and Directives | SI-5 | SI-5 | SI-5 (1) | |
| SI-6 | Security Function Verification | Not Selected | SI-6 | SI-6 | |
| SI-7 | Software, Firmware and Information Integrity | Not Selected | SI-7 (1) (7) | SI-7 (1) (2) (5) (7) (14) | |
| SI-8 | Spam Protection | Not Selected | SI-8 (1) (2) | SI-8 (1) (2) | |
| SI-10 | Information Input Validation | Not Selected | SI-10 | SI-10 | |
| SI-11 | Error Handling | Not Selected | SI-11 | SI-11 | |
| SI-12 | Information Handling and Retention | SI-12 | SI-12 | SI-12 | |
| SI-16 | Memory Protection | SI-16 | SI-16 | SI-16 | |

Note: The -1 Controls (AC-1, AU-1, SC-1, etc.) cannot be inherited and must be provided in some way by the service provider.

The definitions in Table 13‑2 Control Origination and Definitions indicate where each security control originates.

*Table 13‑2. Control Origination and Definitions*

| *Control Origination* | *Definition* | *Example* |
| --- | --- | --- |
| Service Provider Corporate | A control that originates from the Microsoft corporate network. | DNS from the corporate network provides address resolution services for the information system and the service offering. |
| Service Provider System Specific | A control specific to a particular system at Microsoft and the control is not part of the standard corporate controls. | A unique host-based intrusion detection system (HIDs) is available on the service offering platform but is not available on the corporate network. |
| Service Provider Hybrid | A control that makes use of both corporate controls and additional controls specific to a particular system at the Microsoft. | There are scans of the corporate network infrastructure; scans of databases and web-based application are system specific. |
| Configured by Customer | A control where the customer needs to apply a configuration in order to meet the control requirement. | User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http\* or https, etc.), entering an IP range specific to their organization are configurable by the customer. |
| Provided by Customer | A control where the customer needs to provide additional hardware or software in order to meet the control requirement. | The customer provides a SAML SSO solution to implement two-factor authentication. |
| Shared | A control that is managed and implemented partially by the Microsoft and partially by the customer. | Security awareness training must be conducted by both the CSPN and the customer. |
| Inherited from pre-existing FedRAMP Authorization | A control that is inherited from another Microsoft system that has already received a FedRAMP Authorization. | A PaaS or SaaS provider inherits PE controls from an IaaS provider. |

\*Hyper Text Transport Protocol (http)

*Responsible Role* indicates the role of CSP employee who can best respond to questions about the particular control that is described.

## Access Control (AC)

AC-1 Access Control Policy and Procedures Requirements (H)

The organization:

1. Develops, documents, and disseminates to [*FedRAMP Assignment: organization-defined personnel or roles*]:
   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
2. Reviews and updates the current:
   1. Access control policy [*FedRAMP Assignment: at least annually]*; and
   2. Access control procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| AC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_1\_role}} | |
| Parameter AC-01(a): {{ac\_1\_a\_parameter}} | |
| Parameter AC-01(b)(1): {{ac\_1\_b\_1\_parameter}} | |
| Parameter AC-01(b)(2): {{ac\_1\_b\_2\_parameter}} | |
| {{ac\_1\_status}} | |
| {{ac\_1\_origination}} | |

| AC-1 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_1\_a\_implementation}} |
| **Part b** | {{ac\_1\_b\_implementation}} |

AC-2 Account Management (H)

The organization:

1. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];
2. Assigns account managers for information system accounts;
3. Establishes conditions for group and role membership;
4. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
5. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
6. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];
7. Monitors the use of information system accounts;
8. Notifies account managers:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes;
9. Authorizes access to the information system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions/business functions;
10. Reviews accounts for compliance with account management requirements [*FedRAMP Assignment: monthly for privileged access, every six (6) months for non-privileged access*]; and
11. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

| AC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_2\_role}} | |
| Parameter AC-02(a): {{ac\_2\_a\_parameter}} | |
| Parameter AC-02(e):{{ac\_2\_e\_parameter}} | |
| Parameter AC-02(f): {{ac\_2\_f\_parameter}} | |
| Parameter AC-02(j): {{ac\_2\_j\_parameter}} | |
| {{ac\_2\_status}} | |
| {{ac\_2\_origination}} | |

| AC-2 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_2\_a\_implementation}} |
| **Part b** | {{ac\_2\_b\_implementation}} |
| **Part c** | {{ac\_2\_c\_implementation}} |
| **Part d** | {{ac\_2\_d\_implementation}} |
| **Part e** | {{ac\_2\_e\_implementation}} |
| **Part f** | {{ac\_2\_f\_implementation}} |
| **Part g** | {{ac\_2\_g\_implementation}} |
| **Part h** | {{ac\_2\_h\_implementation}} |
| **Part i** | {{ac\_2\_i\_implementation}} |
| **Part j** | {{ac\_2\_j\_implementation}} |
| **Part k** | {{ac\_2\_k\_implementation}} |

AC-2 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to support the management of information system accounts.

| AC-2(1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_2\_1\_role}} | |
| {{ac\_2\_1\_status}} | |
| {{ac\_2\_1\_origination}} | |

|  |
| --- |
| AC-2 (1) What is the solution and how is it implemented? |
| {{ac\_2\_1\_implementation}} |

AC-2 (2) Control ENHANCEMENT (H)

The information system automatically [*FedRAMP Selection: disables*] temporary and emergency accounts after [*FedRAMP Assignment: 24 hours from last use*]

| AC-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_2\_2\_role}} | |
| Parameter AC-2(2)1: {{ac\_2\_2\_1\_parameter}} | |
| Parameter AC-2(2)2: {{ac\_2\_2\_2\_parameter}} | |
| {{ac\_2\_2\_status}} | |
| {{ac\_2\_2\_origination}} | |

|  |
| --- |
| AC-2 (2) What is the solution and how is it implemented? |
| {{ac\_2\_2\_implementation}} |

AC-2 (3) Control ENHANCEMENT (H)

The information system automatically disables inactive accounts after [*FedRAMP Assignment: thirty-five (35) days for user accounts*].

**AC-2 (3) Additional FedRAMP Requirements and Guidance:**

**Requirement**: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the JAB/AO. Where user management is a function of the service, reports of activity of consumer users shall be made available.

| AC-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: {{ac\_2\_3\_role}} | |
| Parameter AC-02(3):{{ac\_2\_3\_parameter}} | |
| {{ac\_2\_3\_status}} | |
| {{ac\_2\_3\_origination}} | |

|  |
| --- |
| AC-2 (3) What is the solution and how is it implemented |
| {{ac\_2\_3\_implementation}} |

AC-2 (4) Control ENHANCEMENT (H)

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [*FedRAMP Assignment: organization and/or service provider system owner*]

| AC-2 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_2\_4\_role}} | |
| Parameter AC-02(4):{{ac\_2\_4\_parameter}} | |
| {{ac\_2\_4\_status}} | |
| {{ac\_2\_4\_origination}} | |

|  |
| --- |
| AC-2 (4) What is the solution and how is it implemented? |
| {{ac\_2\_4\_implementation}} |

AC-2 (5) Control ENHANCEMENT (H)

The organization requires that users log out when [*FedRAMP Assignment: inactivity is anticipated to exceed fifteen (15) minutes*].

**AC-2 (5) Additional FedRAMP Requirements and Guidance:**

**Guidance**: Should use a shorter timeframe than AC-12

| AC-2 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_2\_5\_role}} | |
| Parameter AC-02(5): {{ac\_2\_5\_parameter}} | |
| {{ac\_2\_5\_status}} | |
| {{ac\_2\_5\_origination}} | |

|  |
| --- |
| AC-2 (5) What is the solution and how is it implemented? |
| {{ac\_2\_5\_implementation}} |

AC-2 (7) Control Enhancement (H)

The organization:

1. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
2. Monitors privileged role assignments; and
3. Takes [*FedRAMP* *Assignment: disables//revokes access within an organization-specified timeframe*] when privileged role assignments are no longer appropriate.

|  |  |
| --- | --- |
| AC-2 (7) | Control Summary Information |
| Responsible Role: {{ac\_2\_7\_role}} | |
| Parameter AC-02(7)(c):{{ac\_2\_7\_parameter}} | |
| {{ac\_2\_7\_status}} | |
| {{ac\_2\_7\_origination}} | |

| AC-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_2\_7\_a\_implementation}} |
| **Part b** | {{ac\_2\_7\_b\_implementation}} |
| **Part c** | {{ac\_2\_7\_c\_implementation}} |

AC-2 (9) Control ENHANCEMENT (H)

The organization only permits the use of shared/group accounts that meet [*FedRAMP Assignment: organization-defined need with justification statement that explains why such accounts are necessary*].

**AC-2 (9) Additional FedRAMP Requirements and Guidance**: Required if shared/group accounts are deployed.

| AC-2 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_2\_9\_role}} | |
| Parameter AC-02(9): {{ac\_2\_9\_parameter}} | |
| {{ac\_2\_9\_status}} | |
| {{ac\_2\_9\_origination}} | |

|  |
| --- |
| AC-2 (9) What is the solution and how is it implemented? |
| {{ac\_2\_9\_implementation}} |

AC-2 (10) Control Enhancement (M) (H)

The information system terminates shared/group account credentials when members leave the group.

**AC-2 (10) Additional FedRAMP Requirements and Guidance:** Required if shared/group accounts are deployed.

| AC-2 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_2\_10\_role}} | |
| {{ac\_2\_10\_status}} | |
| {{ac\_2\_10\_origination}} | |

|  |
| --- |
| AC-2 (10) What is the solution and how is it implemented? |
| {{ac\_2\_10\_implementation}} |

AC-2 (11) Control Enhancement (H)

The information system enforces [*Assignment: organization-defined circumstances and/or usage conditions*] for [*Assignment: organization-defined information system accounts*].

| AC-2 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_2\_11\_role}} | |
| Parameter AC-2 (11)-1: {{ac\_2\_11\_1\_parameter}} | |
| Parameter AC-2 (11)-2: {{ac\_2\_11\_2\_parameter}} | |
| {{ac\_2\_11\_status}} | |
| {{ac\_2\_11\_origination}} | |

| AC-2 (11) What is the solution and how is it implemented? |
| --- |
| {{ac\_2\_11\_implementation}} |

AC-2 (12) Control Enhancement (H)

The organization:

1. Monitors information system accounts for [*Assignment: organization-defined atypical use*]; and
2. Reports atypical usage of information system accounts to [*FedRAMP Assignment: at a minimum, the ISSO and/or similar role within the organization*] .

**AC-2 (12) (a) and AC-2 (12) (b) Additional FedRAMP Requirements and Guidance:** Required for privileged accounts.

| AC-2 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_2\_12\_role}} | |
| Parameter AC-02(12)(a):{{ac\_2\_12\_a\_parameter}} | |
| Parameter AC-02(12)(b):{{ac\_2\_12\_b\_parameter}} | |
| {{ac\_2\_12\_status}} | |
| {{ac\_2\_12\_origination}} | |

| AC-2 (12) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_2\_12\_a\_implementation}} |
| **Part b** | {{ac\_2\_12\_b\_implementation}} |

AC-2 (13) Control Enhancement (H)

The organization disables accounts of users posing a significant risk within [*FedRAMP* *Assignment: one (1) hour*] of discovery of the risk.

| AC-2 (13) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_2\_13\_role}} | |
| Parameter AC-2 (13): {{ac\_2\_13\_parameter}} | |
| {{ac\_2\_13\_status}} | |
| {{ac\_2\_13\_origination}} | |

| AC-2 (13) What is the solution and how is it implemented? |
| --- |
| {{ac\_2\_13\_implementation}} |

AC-3 Access Enforcement (L) (M) (H)

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

| AC-3 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_3\_role}} | |
| {{ac\_3\_status}} | |
| {{ac\_3\_origination}} | |

| AC-3 What is the solution and how is it implemented? |
| --- |
| {{ac\_3\_implementation}} |

AC-4 Information Flow Enforcement (M) (H)

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

| AC-4 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_4\_role}} | |
| Parameter AC-04: {{ac\_4\_parameter}} | |
| {{ac\_4\_status}} | |
| {{ac\_4\_origination}} | |

| AC-4 What is the solution and how is it implemented? |
| --- |
| {{ac\_4\_implementation}} |

AC-4 (8) Control Enhancement (H)

The information system enforces information flow control using [*Assignment: organization-defined security policy filters*] as a basis for flow control decisions for [*Assignment: organization-defined information flows*].

| AC-4 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_4\_8\_role}} | |
| Parameter AC-4 (8)-1: {{ac\_4\_8\_1\_parameter}} | |
| Parameter AC-4 (8)-2: {{ac\_4\_8\_2\_parameter}} | |
| {{ac\_4\_8\_status}} | |
| {{ac\_4\_8\_origination}} | |

| AC-4 (8) What is the solution and how is it implemented? |
| --- |
| {{ac\_4\_8\_implementation}} |

AC-4 (21) Control Enhancement (M) (H)

The information system separates 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: {{ac\_4\_21\_role}} | |
| Parameter AC-4(21)-1: {{ac\_4\_21\_1\_parameter}} | |
| Parameter AC-4(21)-2: {{ac\_4\_21\_2\_parameter}} | |
| {{ac\_4\_21\_status}} | |
| {{ac\_4\_21\_origination}} | |

| AC-4 (21) What is the solution and how is it implemented? |
| --- |
| {{ac\_4\_21\_implementation}} |

AC-5 Separation of Duties (M) (H)

The organization:

Separates [Assignment: organization-defined duties of individuals];

Documents separation of duties of individuals; and

Defines information system access authorizations to support separation of duties.

**AC-5 Additional FedRAMP Requirements and Guidance:**

**Guidance**: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP. Directions for attaching the Separation of Duties Matrix document may be found in Section 15.11 Attachment 11, Separation of Duties Matrix.

| AC-5 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_5\_role}} | |
| Parameter AC-05(a): {{ac\_5\_parameter}} | |
| {{ac\_5\_status}} | |
| {{ac\_5\_origination}} | |

| AC-5 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_5\_a\_implementation}} |
| **Part b** | {{ac\_5\_b\_implementation}} |
| **Part c** | {{ac\_5\_c\_implementation}} |

AC-6 Least Privilege (M) (H)

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

| AC-6 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_6\_role}} | |
| {{ac\_6\_status}} | |
| {{ac\_6\_origination}} | |

| AC-6 What is the solution and how is it implemented? |
| --- |
| {{ac\_6\_implementation}} |

AC-6 (1) Control Enhancement (H)

The organization explicitly authorizes access to [*FedRAMP Assignment: all functions not publicly accessible and all security-relevant information not publicly available*].

| AC-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_6\_1\_role}} | |
| Parameter AC-06(1): {{ac\_6\_1\_parameter}} | |
| {{ac\_6\_1\_status}} | |
| {{ac\_6\_1\_origination}} | |

| AC-6 (1) What is the solution and how is it implemented? |
| --- |
| {{ac\_6\_1\_implementation}} |

AC-6 (2) Control Enhancement (M) (H)

The organization requires that users of information system accounts, or roles, with access to [*FedRAMP Assignment: all security functions*], use non-privileged accounts or roles, when accessing non-security functions.

**AC-6 (2) Additional FedRAMP Requirements and Guidance:** Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.

| AC-6 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_6\_2\_role}} | |
| Parameter AC-06(2): {{ac\_6\_2\_parameter}} | |
| {{ac\_6\_2\_status}} | |
| {{ac\_6\_2\_origination}} | |

| AC-6 (2) What is the solution and how is it implemented? |
| --- |
| {{ac\_6\_2\_implementation}} |

AC-6 (3) Control Enhancement (H)

The organization authorizes network access to [*FedRAMP Assignment: all privileged commands*] only for [*Assignment: organization-defined compelling operational needs*] and documents the rationale for such access in the security plan for the information system.

| AC-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_6\_3\_role}} | |
| Parameter AC-6 (3)-1: {{ac\_6\_3\_1\_parameter}} | |
| Parameter AC-6 (3)-2: {{ac\_6\_3\_2\_parameter}} | |
| {{ac\_6\_3\_status}} | |
| {{ac\_6\_3\_origination}} | |

| AC-6 (3) What is the solution and how is it implemented? |
| --- |
| {{ac\_6\_3\_implementation}} |

AC 6 (5) Control Enhancement (M) (H)

The organization restricts privileged accounts on the information system to [*Assignment: organization-defined personnel or roles*].

| AC-6 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_6\_5\_role}} | |
| Parameter AC-06(5): {{ac\_6\_5\_parameter}} | |
| {{ac\_6\_5\_status}} | |
| {{ac\_6\_5\_origination}} | |

| AC-6 (5) What is the solution and how is it implemented? |
| --- |
| {{ac\_6\_5\_implementation}} |

AC-6 (7) Control Enhancement (H)

The organization:

1. Reviews [*FedRAMP* *Assignment: at a minimum, annually*] the privileges assigned to [*FedRAMP* *Assignment: all users with privileges* to validate the need for such privileges; and
2. Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

| AC-6 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_6\_7\_role}} | |
| Parameter AC-6(7)(a)-1: {{ac\_6\_7\_1\_parameter}} | |
| Parameter AC-6(7)(a)-2: {{ac\_6\_7\_2\_parameter}} | |
| {{ac\_6\_7\_status}} | |
| {{ac\_6\_7\_origination}} | |

| AC-6 (7) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_6\_7\_a\_implementation}} |
| **Part b** | {{ac\_6\_7\_b\_implementation}} |

AC-6 (8) Control Enhancement (H)

The information system prevents [*FedRAMP Assignment: any software except software explicitly documented*] from executing at higher privilege levels than users executing the software.

| AC-6 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_6\_8\_role}} | |
| Parameter AC-6 (8): {{ac\_6\_8\_parameter}} | |
| {{ac\_6\_8\_status}} | |
| {{ac\_6\_8\_origination}} | |

| AC-6 (8) What is the solution and how is it implemented? |
| --- |
| {{ac\_6\_8\_implementation}} |

AC-6 (9) Control Enhancement (M) (H)

The information system audits the execution of privileged functions.

| AC-6 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_6\_9\_role}} | |
| {{ac\_6\_9\_status}} | |
| {{ac\_6\_9\_origination}} | |

| AC-6 (9) What is the solution and how is it implemented? |
| --- |
| {{ac\_6\_9\_implementation}} |

AC-6 (10) Control Enhancement (M) (H)

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

| AC-6 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_6\_10\_role}} | |
| {{ac\_6\_10\_status}} | |
| {{ac\_6\_10\_origination}} | |

| AC-6 (10) What is the solution and how is it implemented? |
| --- |
| {{ac\_6\_10\_implementation}} |

AC-7 Unsuccessful Login Attempts (H)

The organization:

Enforces a limit of [*FedRAMP Assignment: not more than three (3)*] consecutive invalid logon attempts by a user during a [*FedRAMP Assignment: fifteen (15) minutes*]; and

Automatically [*Selection: locks the account/node for a* [*FedRAMP Assignment: minimum of three (3) hours or until unlocked by an administrator*; *delays next logon prompt according to* [*Assignment: organization-defined delay algorithm*] when the maximum number of unsuccessful attempts is exceeded.

| AC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_7\_role}} | |
| Parameter AC-7(a)-1: {{ac\_7\_a\_1\_parameter}} | |
| Parameter AC-7(a)-2: {{ac\_7\_a\_2\_parameter}} | |
| Parameter AC-7(b)-1: {{ac\_7\_b\_1\_parameter}} | |
| Parameter AC-7(b)-2: {{ac\_7\_b\_2\_parameter}} | |
| {{ac\_7\_status}} | |
| {{ac\_7\_origination}} | |

| AC-7 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_7\_a\_implementation}} |
| **Part b** | {{ac\_7\_b\_implementation}} |

AC-7 (2) Control Enhancement (H)

The information system purges/wipes information from [*FedRAMP Assignment: mobile devices as defined by organization policy*] based on [*Assignment: organization-defined purging/wiping requirements/techniques*] after [*FedRAMP Assignment: three (3)*] consecutive, unsuccessful device logon attempts.

| AC-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_7\_2\_role}} | |
| Parameter AC-7 (2)-1: {{ac\_7\_2\_1\_parameter}} | |
| Parameter AC-7 (2)-2: {{ac\_7\_2\_2\_parameter}} | |
| Parameter AC-7 (2)-3: {{ac\_7\_2\_3\_parameter}} | |
| {{ac\_7\_2\_status}} | |
| {{ac\_7\_2\_origination}} | |

| AC-7 (2) What is the solution and how is it implemented? |
| --- |
| {{ac\_7\_2\_implementation}} |

AC-8 System Use Notification (L) (M) (H)

The information system:

1. Displays to users [*Assignment: organization-defined system use notification message or banner (FedRAMP Assignment: see additional Requirements and Guidance)*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
   1. Users are accessing a U.S. Government information system;
   2. Information system usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
   4. Use of the information system indicates consent to monitoring and recording;
2. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
3. For publicly accessible systems:
   1. Displays system use information [*Assignment: organization-defined conditions (FedRAMP Assignment: see additional Requirements and Guidance)*], before granting further access;
   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Includes a description of the authorized uses of the system.

**AC-8 Additional FedRAMP Requirements and Guidance**:

**Requirement:** The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

**Requirement:** The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO.

**Guidance:** If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

**Requirement:** If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

| AC-8 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_8\_role}} | |
| Parameter AC-08(a):{{ac\_8\_a\_parameter}} | |
| Parameter AC-08(c)(1):{{ac\_8\_c\_1\_parameter}} | |
| {{ac\_8\_status}} | |
| {{ac\_8\_origination}} | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_8\_a\_implementation}} |
| **Part b** | {{ac\_8\_b\_implementation}} |
| **Part c** | {{ac\_8\_c\_implementation}} |

**Additional FedRAMP Requirements and Guidance**

**Requirement 1**: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

**Requirement 2**: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO. If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

**Requirement 3**: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

| AC-8 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_8\_r\_role}} | |
| {{ac\_8\_r\_status}} | |
| {{ac\_8\_r\_origination}} | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| **Req. 1** | {{ac\_8\_r\_1\_implementation}} |
| **Req. 2** | {{ac\_8\_r\_2\_implementation}} |
| **Req. 3** | {{ac\_8\_r\_3\_implementation}} |

AC-10 Concurrent Session Control (M) (H)

The information system limits the number of concurrent sessions for each [*Assignment: organization-defined account and/or account type*] to [*FedRAMP Assignment: three (3) sessions for privileged access and two (2) sessions for non-privileged access*].

| AC-10 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_10\_role}} | |
| Parameter AC-10-1: {{ac\_10\_1\_parameter}} | |
| Parameter AC-10-2: {{ac\_10\_2\_parameter}} | |
| {{ac\_10\_status}} | |
| {{ac\_10\_origination}} | |

| AC-10 What is the solution and how is it implemented? |
| --- |
| {{ac\_10\_implementation}} |

AC-11 Session Lock (M) (H)

The information system:

1. Prevents further access to the system by initiating a session lock after [*FedRAMP Assignment: fifteen (15) minutes*] of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

| AC-11 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_11\_role}} | |
| Parameter AC-11(a): {{ac\_11\_a\_parameter}} | |
| {{ac\_11\_status}} | |
| {{ac\_11\_origination}} | |

| AC-11 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_11\_a\_implementation}} |
| **Part b** | {{ac\_11\_b\_implementation}} |

AC-11 (1) Control Enhancement (M) (H)

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

| AC-11 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_11\_1\_role}} | |
| {{ac\_11\_1\_status}} | |
| {{ac\_11\_1\_origination}} | |

| AC-11 (1) What is the solution and how is it implemented? |
| --- |
| {{ac\_11\_1\_implementation}} |

AC-12 Session Termination (M) (H)

The information system automatically terminates a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

| AC-12 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_12\_role}} | |
| Parameter AC-12: {{ac\_12\_parameter}} | |
| {{ac\_12\_status}} | |
| {{ac\_12\_origination}} | |

| AC-12 What is the solution and how is it implemented? |
| --- |
| {{ac\_12\_implementation}} |

AC-12 (1) Control Enhancement (H)

The information system:

1. Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [*Assignment: organization-defined information resources*]; and
2. Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

**AC-12(1) Additional FedRAMP Requirements and Guidance**:

**Guidance:** Testing for logout functionality (OTG-SESS-006) https://www.owasp.org/index.php/Testing\_for\_logout\_functionality\_%28OTG-SESS-006%29

| AC-12 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_12\_1\_role}} | |
| Parameter AC-12(1)(a)1: {{ac\_12\_1\_a\_1\_parameter}} | |
| {{ac\_12\_1\_status}} | |
| {{ac\_12\_1\_origination}} | |

| AC-12 (1) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_12\_1\_a\_implementation}} |
| **Part b** | {{ac\_12\_1\_b\_implementation}} |

AC-14 Permitted Actions without Identification or Authentication (L) (M) (H)

The organization:

1. Identifies [*Assignment: organization-defined user actions*] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
2. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

| AC-14 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_14\_role}} | |
| Parameter AC-14(a): {{ac\_14\_a\_parameter}} | |
| {{ac\_14\_status}} | |
| {{ac\_14\_origination}} | |

| AC-14 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_14\_a\_implementation}} |
| **Part b** | {{ac\_14\_b\_implementation}} |

AC-17 Remote Access (L) (M) (H)

The organization:

1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
2. Authorizes remote access to the information system prior to allowing such connections.

| AC-17 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_17\_role}} | |
| {{ac\_17\_status}} | |
| {{ac\_17\_origination}} | |

| AC-17 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_17\_a\_implementation}} |
| **Part b** | {{ac\_17\_b\_implementation}} |

AC-17 (1) Control Enhancement (M) (H)

The information system monitors and controls remote access methods.

| AC-17 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_17\_1\_role}} | |
| {{ac\_17\_1\_status}} | |
| {{ac\_17\_1\_origination}} | |

| AC-17 (1) What is the solution and how is it implemented? |
| --- |
| {{ac\_17\_1\_implementation}} |

AC-17 (2) Control Enhancement (M) (H)

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

| AC-17 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_17\_2\_role}} | |
| {{ac\_17\_2\_status}} | |
| {{ac\_17\_2\_origination}} | |

| AC-17 (2) What is the solution and how is it implemented? |
| --- |
| {{ac\_17\_2\_implementation}} |

AC-17 (3) Control Enhancement (M) (H)

The information system routes all remote accesses through [*Assignment: organization-defined number*] managed network access control points.

| AC-17 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_17\_3\_role}} | |
| Parameter AC-17(3): {{ac\_17\_3\_parameter}} | |
| {{ac\_17\_3\_status}} | |
| {{ac\_17\_3\_origination}} | |

| AC-17 (3) What is the solution and how is it implemented? |
| --- |
| {{ac\_17\_3\_implementation}} |

AC-17 (4) Control Enhancement (M) (H)

The organization:

1. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*Assignment: organization-defined needs*]; and
2. Documents the rationale for such access in the security plan for the information system.

| AC-17 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_17\_4\_role}} | |
| Parameter AC-17(4)(a): {{ac\_17\_4\_a\_parameter}} | |
| {{ac\_17\_4\_status}} | |
| {{ac\_17\_4\_origination}} | |

| AC-17 (4) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_17\_4\_a\_implementation}} |
| **Part b** | {{ac\_17\_4\_b\_implementation}} |

AC-17 (9) Control Enhancement (M) (H)

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [*FedRAMP Assignment: fifteen (15) minutes*].

| AC-17 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_17\_9\_role}} | |
| Parameter AC-17(9): {{ac\_17\_9\_parameter}} | |
| {{ac\_17\_9\_status}} | |
| {{ac\_17\_9\_origination}} | |

| AC-17 (9) What is the solution and how is it implemented? |
| --- |
| {{ac\_17\_9\_implementation}} |

AC-18 Wireless Access Restrictions (L) (M) (H)

The organization:

1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
2. Authorizes wireless access to the information system prior to allowing such connections.

| AC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_18\_role}} | |
| {{ac\_18\_status}} | |
| {{ac\_18\_origination}} | |

| AC-18 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_18\_a\_implementation}} |
| **Part b** | {{ac\_18\_b\_implementation}} |

AC-18 (1) Control Enhancement (M) (H)

The information system protects wireless access to the system using authentication of [*Selection (one or more): users; devices*] and encryption.

| AC-18 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_18\_1\_role}} | |
| Parameter AC-18(1): {{ac\_18\_1\_parameter}} | |
| {{ac\_18\_1\_status}} | |
| {{ac\_18\_1\_origination}} | |

| AC-18 (1) What is the solution and how is it implemented? |
| --- |
| {{ac\_18\_1\_implementation}} |

AC-18 (3) Control Enhancement (H)

The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

| AC-18 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_18\_3\_role}} | |
| {{ac\_18\_3\_status}} | |
| {{ac\_18\_3\_origination}} | |

| AC-18 (3) What is the solution and how is it implemented? |
| --- |
| {{ac\_18\_3\_implementation}} |

AC-18 (4) Control Enhancement (H)

The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

| AC-18 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_18\_4\_role}} | |
| {{ac\_18\_4\_status}} | |
| {{ac\_18\_4\_origination}} | |

| AC-18 (4) What is the solution and how is it implemented? |
| --- |
| {{ac\_18\_4\_implementation}} |

AC-18 (5) Control Enhancement (H)

The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

| AC-18 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_18\_5\_role}} | |
| {{ac\_18\_5\_status}} | |
| {{ac\_18\_5\_origination}} | |

| AC-18 (5) What is the solution and how is it implemented? |
| --- |
| {{ac\_18\_5\_implementation}} |

AC-19 Access Control for Portable and Mobile Systems (L) (M) (H)

The organization:

1. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
2. Authorizes the connection of mobile devices to organizational information systems.

| AC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_19\_role}} | |
| {{ac\_19\_status}} | |
| {{ac\_19\_origination}} | |

| AC-19 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_19\_a\_implementation}} |
| **Part b** | {{ac\_19\_b\_implementation}} |

AC-19 (5) Control Enhancement (M) (H)

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

| AC-19 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_19\_5\_role}} | |
| Parameter AC-19(5)-1: {{ac\_19\_5\_1\_parameter}} | |
| Parameter AC-19(5)-2: {{ac\_19\_5\_2\_parameter}} | |
| {{ac\_19\_5\_status}} | |
| {{ac\_19\_5\_origination}} | |

| AC-19 (5) What is the solution and how is it implemented? | |
| --- | --- |
| **AC-19 (5)** | {{ac\_19\_5\_implementation}} |

AC-20 Use of External Information Systems (L) (M) (H)

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

1. Access the information system from external information systems; and
2. Process, store, or transmit organization-controlled information using external information systems.

| AC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_20\_role}} | |
| {{ac\_20\_status}} | |
| {{ac\_20\_origination}} | |

| AC-20 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_20\_a\_implementation}} |
| **Part b** | {{ac\_20\_b\_implementation}} |

AC-20 (1) Control Enhancement (M) (H)

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

1. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan; or
2. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

| AC-20 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_20\_1\_role}} | |
| {{ac\_20\_1\_status}} | |
| {{ac\_20\_1\_origination}} | |

| AC-20 (1) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_20\_1\_a\_implementation}} |
| **Part b** | {{ac\_20\_1\_b\_implementation}} |

AC-20 (2) Control Enhancement (M) (H)

The organization [*Selection: restricts; prohibits*] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

| AC-20 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_20\_2\_role}} | |
| Parameter AC-20(2): {{ac\_20\_2\_parameter}} | |
| {{ac\_2-\_2\_status}} | |
| {{ac\_20\_2\_origination}} | |

| AC-20 (2) What is the solution and how is it implemented? |
| --- |
| {{ac\_20\_2\_implementation}} |

AC-21 Information Sharing (M) (H)

The organization:

1. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and
2. Employs [*Assignment: organization-defined automated mechanisms or manual processes*] to assist users in making information sharing/collaboration decisions.

| AC-21 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_21\_role}} | |
| Parameter AC-21(a): {{ac\_21\_a\_parameter}} | |
| Parameter AC-21(b): {{ac\_21\_b\_parameter}} | |
| {{ac\_21\_status}} | |
| {{ac\_21\_origination}} | |

| AC-21 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_21\_a\_implementation}} |
| **Part b** | {{ac\_21\_b\_implementation}} |

AC-22 Publicly Accessible Content (L) (M) (H)

The organization:

1. Designates individuals authorized to post information onto a publicly accessible information system;
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
3. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
4. Reviews the content on the publicly accessible information system for nonpublic information [*FedRAMP Assignment: at least quarterly*] and removes such information, if discovered.

| AC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ac\_22\_role}} | |
| Parameter AC-22(d): {{ac\_22\_d\_parameter}} | |
| {{ac\_22\_status}} | |
| {{ac\_22\_origination}} | |

| AC-22 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ac\_22\_a\_implementation}} |
| **Part b** | {{ac\_22\_b\_implementation}} |
| **Part c** | {{ac\_22\_c\_implementation}} |
| **Part d** | {{ac\_22\_d\_implementation}} |

## Awareness and Training (AT)

AT-1 Security Awareness and Training Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
2. Reviews and updates the current:
   1. Security awareness and training policy [*FedRAMP Assignment: at least annually*; and
   2. Security awareness and training procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*]*.*

| AT-1 | Control Summary Information |
| --- | --- |
| Responsible Role: {{at\_1\_role}} | |
| Parameter AT-01(a): {{at\_1\_a\_parameter}} | |
| Parameter AT-01(b)(1): {{at\_1\_b\_1\_parameter}} | |
| Parameter AT-01(b)(2): {{at\_1\_b\_2\_parameter}} | |
| {{at\_1\_status}} | |
| {{at\_1\_origination}} | |

| AT-1 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{at\_1\_a\_implementation}} |
| **Part b** | {{at\_1\_b\_implementation}} |

AT-2 Security Awareness (L) (M) (H)

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

1. As part of initial training for new users;
2. When required by information system changes; and
3. [*FedRAMP Assignment: at least annually*] thereafter.

| AT-2 | Control Summary Information |
| --- | --- |
| Responsible Role: {{at\_2\_role}} | |
| Parameter AT-02(c): {{at\_2\_c\_parameter}} | |
| {{at\_2\_status}} | |
| {{at\_2\_origination}} | |

| AT-2 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{at\_2\_a\_implementation}} |
| **Part b** | {{at\_2\_b\_implementation}} |
| **Part c** | {{at\_2\_c\_implementation}} |

AT-2 (2) Control Enhancement (M) (H)

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

| AT-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{at\_2\_2\_role}} | |
| {{at\_2\_2\_status}} | |
| {{at\_2\_2\_origination}} | |

| AT-2 (2) What is the solution and how is it implemented? |
| --- |
| {{at\_2\_2\_implementation}} |

AT-3 Role-Based Security Training (L) (M) (H)

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

1. Before authorizing access to the information system or performing assigned duties;
2. When required by information system changes; and
3. [*FedRAMP Assignment: at least annually*] thereafter.

| AT-3 | Control Summary Information |
| --- | --- |
| Responsible Role: {{at\_3\_role}} | |
| Parameter AT-03(c): {{at\_3\_c\_parameter}} | |
| {{at\_3\_status}} | |
| {{at\_3\_origination}} | |

| AT-3 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{at\_3\_a\_implementation}} |
| **Part b** | {{at\_3\_b\_implementation}} |
| **Part c** | {{at\_3\_c\_implementation}} |

AT-3 (3) Control Enhancement (H)

The organization includes practical exercises in security training that reinforce training objectives.

| AT-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{at\_3\_3\_role}} | |
| {{at\_3\_3\_status}} | |
| {{at\_3\_3\_origination}} | |

| AT-3 (3) What is the solution and how is it implemented? |
| --- |
| {{at\_3\_3\_implementation}} |

AT-3 (4) Control Enhancement (H)

The organization provides training to its personnel on [*FedRAMP Assignment: malicious code indicators as defined by organization incident policy/capability*] to recognize suspicious communications and anomalous behavior in organizational information systems.

| AT-3 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{at\_3\_4\_role}} | |
| Parameter AT-3 (4): {{at\_3\_4\_parameter}} | |
| {{at\_3\_4\_status}} | |
| {{at\_3\_4\_origination}} | |

| AT-3 (4) What is the solution and how is it implemented? |
| --- |
| {{at\_3\_4\_implementation}} |

AT-4 Security Training Records (H)

The organization:

1. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records for [*FedRAMP Assignment: at least five (5) years or 5 years after completion of a specific training program*].

| AT-4 | Control Summary Information |
| --- | --- |
| Responsible Role: {{at\_4\_role}} | |
| Parameter AT-04(b): {{at\_4\_b\_parameter}} | |
| {{at\_4\_status}} | |
| {{at\_4\_origination}} | |

| AT-4 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{at\_4\_a\_implementation}} |
| **Part b** | {{at\_4\_b\_implementation}} |

## Audit and Accountability (AU)

AU-1 Audit and Accountability Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
2. Reviews and updates the current:
   1. Audit and accountability policy [*FedRAMP Assignment: at least annually*]; and
   2. Audit and accountability procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| AU-1 | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_1\_role}} | |
| Parameter AU-01(a): {{au\_1\_a\_parameter}} | |
| Parameter AU-01(b)(1): {{au\_1\_b\_1\_parameter}} | |
| Parameter AU-01(b)(2): {{au\_1\_b\_2\_parameter}} | |
| {{au\_1\_status}} | |
| {{au\_1\_origination}} | |

| AU-1 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{au\_1\_a\_implementation}} |
| **Part b** | {{au\_1\_b\_implementation}} |

AU-2 Audit Events (L) (M) (H)

The organization:

1. Determines that the information system is capable of auditing the following events: [*FedRAMP Assignment:* [*Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes*];
2. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
3. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
4. Determines that the following events are to be audited within the information system: [*FedRAMP Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited continually for each identified event*.

**AU-2 Additional FedRAMP Requirements and Guidance:**

**Requirement**: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO.

| AU-2 | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_2\_role}} | |
| Parameter AU-02(a): {{au\_2\_a\_parameter}} | |
| Parameter AU-02(d): {{au\_2\_d\_parameter}} | |
| {{au\_2\_status}} | |
| {{au\_2\_origination}} | |

| AU-2 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{au\_2\_a\_implementation}} |
| **Part b** | {{au\_2\_b\_implementation}} |
| **Part c** | {{au\_2\_c\_implementation}} |
| **Part d** | {{au\_2\_d\_implementation}} |

AU-2 (3) Control Enhancement (M) (H)

The organization reviews and updates the audited events [*FedRAMP Assignment: annually or whenever there is a change in the threat environment*].

**AU-2 (3) Additional FedRAMP Requirements and Guidance:**

**Guidance**: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB/AO.

| AU-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_2\_3\_role}} | |
| Parameter AU-02(3): {{au\_2\_3\_parameter}} | |
| {{au\_2\_3\_status}} | |
| {{au\_2\_3\_origination}} | |

| AU-2 (3) What is the solution and how is it implemented? |
| --- |
| {{au\_2\_3\_implementation}} |

AU-3 Content of Audit Records (L) (M) (H)

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

| AU-3 | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_3\_role}} | |
| {{au\_3\_status}} | |
| {{au\_3\_origination}} | |

| AU-3 What is the solution and how is it implemented? |
| --- |
| {{au\_3\_implementation}} |

AU-3 (1) Control Enhancement (H)

The information system generates audit records containing the following additional information: [*FedRAMP Assignment: organization-defined additional, more detailed information].*

**AU-3 (1) Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider defines audit record types [*FedRAMP Assignment: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon; individual identities of group account users; full-text of privileged commands*]. The audit record types are approved and accepted by the JAB/AO.

**Guidance:** For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.

| AU-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_3\_1\_role}} | |
| Parameter AU-03(1): {{au\_3\_1\_parameter}} | |
| {{au\_3\_1\_status}} | |
| {{au\_3\_1\_origination}} | |

| AU-3 (1) What is the solution and how is it implemented? |
| --- |
| {{au\_3\_1\_implementation}} |

AU-3 (2) Control Enhancement (H)

The information system provides centralized management and configuration of the content to be captured in audit records generated by [*FedRAMP Assignment: all network, data storage, and computing devices*].

| AU-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_3\_2\_role}} | |
| Parameter AU-3 (2): {{au\_3\_2\_parameter}} | |
| {{au\_3\_2\_status}} | |
| {{au\_3\_2\_origination}} | |

| AU-3 (2) What is the solution and how is it implemented? |
| --- |
| {{au\_3\_2\_implementation}} |

AU-4 Audit Storage Capacity (L) (M) (H)

The organization allocates audit record storage capacity in accordance with [*Assignment: organization-defined audit record storage requirements*].

| AU-4 | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_4\_role}} | |
| Parameter AU-04: {{au\_4\_parameter}} | |
| {{au\_4\_status}} | |
| {{au\_4\_origination}} | |

| AU-4 What is the solution and how is it implemented? |
| --- |
| {{au\_4\_implementation}} |

AU-5 Response to Audit Processing Failures (L) (M) (H)

The information system:

1. Alerts [*Assignment: organization-defined personnel or roles*] in the event of an audit processing failure; and
2. Takes the following additional actions: [*FedRAMP Assignment: organization-defined actions to be taken; (overwrite oldest record)*].

| AU-5 | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_5\_role}} | |
| Parameter AU-05(a): {{au\_5\_a\_parameter}} | |
| Parameter AU-05(b): {{au\_5\_parameter}} | |
| {{au\_5\_status}} | |
| {{au\_5\_origination}} | |

| AU-5 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{au\_5\_a\_implementation}} |
| **Part b** | {{au\_5\_b\_implementation}} |

AU-5 (1) Control Enhancement (H)

The information system provides a warning to [*Assignment: organization-defined personnel, roles, and/or locations*] within [*Assignment: organization-defined time period*] when allocated audit record storage volume reaches [*Assignment: organization-defined percentage*] of repository maximum audit record storage capacity.

| AU-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_5\_1\_role}} | |
| Parameter AU-5 (1)-1: {{au\_5\_1\_1\_parameter}} | |
| Parameter AU-5 (1)-2: {{au\_5\_1\_2\_parameter}} | |
| Parameter AU-5 (1)-3: {{au\_5\_1\_3\_parameter}} | |
| {{au\_5\_1\_status}} | |
| {{au\_5\_1\_origination}} | |

| AU-5 (1) What is the solution and how is it implemented? |
| --- |
| {{au\_5\_1\_implementation}} |

AU-5 (2) Control Enhancement (H)

The information system provides an alert in [*FedRAMP Assignment: organization-defined real-time*] to [*FedRAMP Assignment: service provider personnel with authority to address failed audit events*] when the following audit failure events occur: [*FedRAMP Assignment:* *audit failure events requiring real-time alerts, as defined by organization audit policy*].

| AU-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_5\_2\_role}} | |
| Parameter AU-5 (2)-1: {{au\_5\_2\_1\_parameter}} | |
| Parameter AU-5 (2)-2: {{au\_5\_2\_2\_parameter}} | |
| Parameter AU-5 (2)-3: {{au\_5\_2\_3\_parameter}} | |
| {{au\_5\_2\_status}} | |
| {{au\_5\_2\_origination}} | |

| AU-5 (2) What is the solution and how is it implemented? |
| --- |
| {{au\_5\_2\_implementation}} |

AU-6 Audit Review, Analysis, and Reporting (L) (M) (H)

The organization:

1. Reviews and analyzes information system audit records [*FedRAMP Assignment: at least weekly*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and
2. Reports findings to [*FedRAMP Assignment: organization-defined personnel or roles*].

**AU-6 Additional FedRAMP Requirements and Guidance:**

**Requirement:** Coordination between service provider and consumer shall be documented and accepted by the Authorizing Official. In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented.

| AU-6 | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_6\_role}} | |
| Parameter AU-6(a)-1: {{au\_6\_a\_1\_parameter}} | |
| Parameter AU-6(a)-2: {{au\_6\_a\_2\_parameter}} | |
| Parameter AU-6(b): {{au\_6\_b\_parameter}} | |
| {{au\_6\_status}} | |
| {{au\_6\_origination}} | |

| AU-6 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{au\_6\_a\_implementation}} |
| **Part b** | {{au\_6\_b\_implementation}} |

AU-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

| AU-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_6\_1\_role}} | |
| {{au\_6\_1\_status}} | |
| {{au\_6\_1\_origination}} | |

| AU-6 (1) What is the solution and how is it implemented? |
| --- |
| {{au\_6\_1\_implementation}} |

AU-6 (3) Control Enhancement (M) (H)

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

| AU-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_6\_3\_role}} | |
| {{au\_6\_3\_status}} | |
| {{au\_6\_3\_origination}} | |

| AU-6 (3) What is the solution and how is it implemented? |
| --- |
| {{au\_6\_3\_implementation}} |

AU-6 (4) Control Enhancement (H)

The information system provides the capability to centrally review and analyze audit records from multiple components within the system.

| AU-6 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_6\_4\_role}} | |
| {{au\_6\_4\_status}} | |
| {{au\_6\_4\_origination}} | |

| AU-6 (4) What is the solution and how is it implemented? |
| --- |
| {{au\_6\_4\_implementation}} |

AU-6 (5) Control Enhancement (H)

The organization integrates analysis of audit records with analysis of [*FedRAMP* *Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; penetration test data;* [*Assignment: organization-defined data/information collected from other sources*]] to further enhance the ability to identify inappropriate or unusual activity.

| AU-6 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_6\_5\_role}} | |
| Parameter AU-6 (5): {{au\_6\_5\_parameter}} | |
| {{au\_6\_5\_status}} | |
| {{au\_6\_5\_origination}} | |

| AU-6 (5) What is the solution and how is it implemented? |
| --- |
| {{au\_6\_5\_implementation}} |

AU-6 (6) Control Enhancement (H)

The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

**AU-6 Additional FedRAMP Requirements and Guidance:**

**Requirement:** Coordination between service provider and consumer shall be documented and accepted by the JAB/AO.

| AU-6 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_6\_6\_role}} | |
| {{au\_6\_6\_status}} | |
| {{au\_6\_6\_origination}} | |

| AU-6 (6) What is the solution and how is it implemented? |
| --- |
| {{au\_6\_6\_implementation}} |

AU-6 (7) Control Enhancement (H)

The organization specifies the permitted actions for each [*FedRAMP Selection (one or more): information system process; role; user*] associated with the review, analysis, and reporting of audit information.

| AU-6 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_6\_7\_role}} | |
| Parameter AU-6 (7): {{au\_6\_7\_parameter}} | |
| {{au\_6\_7\_status}} | |
| {{au\_6\_7\_origination}} | |

| AU-6 (7) What is the solution and how is it implemented? |
| --- |
| {{au\_6\_7\_implementation}} |

AU-6 (10) Control Enhancement (H)

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

| AU-6 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_6\_10\_role}} | |
| {{au\_6\_10\_status}} | |
| {{au\_6\_10\_origination}} | |

| AU-6 (10) What is the solution and how is it implemented? |
| --- |
| {{au\_6\_10\_implementation}} |

AU-7 Audit Reduction and Report Generation (M) (H)

The information system provides an audit reduction and report generation capability that:

1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
2. Does not alter the original content or time ordering of audit records.

| AU-7 | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_7\_role}} | |
| {{au\_7\_status}} | |
| {{au\_7\_origination}} | |

| AU-7 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{au\_7\_a\_implementation}} |
| **Part b** | {{au\_7\_b\_implementation}} |

AU-7 (1) Control Enhancement (M) (H)

The information system provides the capability to process audit records for events of interest based on [*Assignment: organization-defined audit fields within audit records*].

| AU-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_7\_1\_role}} | |
| Parameter AU-07(1): {{au\_7\_1\_parameter}} | |
| {{au\_7\_1\_status}} | |
| {{au\_7\_1\_origination}} | |
| AU-7 (1) What is the solution and how is it implemented? | |
| {{au\_7\_1\_implementation}} | |

AU-8 Time Stamps (L) (M) (H)

The information system:

1. Uses internal system clocks to generate time stamps for audit records; and
2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*Assignment: one second granularity of time measurement*].

| AU-8 | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_8\_role}} | |
| Parameter AU-08(b): {{au\_8\_b\_parameter}} | |
| {{au\_8\_status}} | |
| {{au\_8\_origination}} | |

| AU-8 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{au\_8\_a\_implementation}} |
| **Part b** | {{au\_8\_b\_implementation}} |

AU-8 (1) Control Enhancement (M) (H)

The information system:

1. Compares the internal information system clocks with [*FedRAMP Assignment: authoritative time source:* [[*http://tf.nist.gov/tf-cgi/servers.cgi*](http://tf.nist.gov/tf-cgi/servers.cgi)] [*at least hourly]*]; and
2. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [*Assignment: organization-defined time period*].

| AU-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_8\_1\_role}} | |
| Parameter AU-8(1)(a)-1: {{au\_8\_1\_a\_1\_parameter}} | |
| Parameter AU-8(1)(a)-2: {{au\_8\_1\_a\_2\_parameter}} | |
| Parameter AU-8(1)(b): {{au\_8\_1\_b\_parameter}} | |
| {{au\_8\_1\_status}} | |
| {{au\_8\_1\_origination}} | |

| AU-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{au\_8\_1\_a\_implementation}} |
| **Part b** | {{au\_8\_1\_b\_implementation}} |

**AU-8 (1) Additional FedRAMP Requirements and Guidance:**

**Requirement**: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.

**Requirement**: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.

**Guidance**: The service provider selects primary and secondary time servers used by the NIST Internet time service, or by a Stratum-1 time server. The secondary server is selected from a different geographic region than the primary server.

If using Windows Active Directory, all servers should synchronize time with the time source for the Windows Domain Controller. If using some other directory services (e.g., LDAP), all servers should synchronize time with the time source for the directory server. Synchronization of system clocks improves the accuracy of log analysis.

| AU-8 (1) Req. | Additional Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: {{au\_8\_1\_r\_role}} | |
| Parameter AU-8(1)(a)-1: {{au\_8\_1\_a\_1\_r\_parameter}} | |
| Parameter AU-8(1)(a)-2: {{au\_8\_1\_a\_2\_r\_parameter}} | |
| Parameter AU-8(1)(b): {{au\_8\_1\_b\_r\_parameter}} | |
| {{au\_8\_1\_r\_status}} | |
| {{au\_8\_1\_r\_origination}} | |

| AU-8 (1) Req. What is the solution and how is it implemented? | |
| --- | --- |
| **Req. 1** | {{au\_8\_1\_r\_1\_implementation}} |
| **Req. 2** | {{au\_8\_1\_r\_2\_implementation}} |

AU-9 Protection of Audit Information (L) (M) (H)

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

| AU-9 | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_9\_role}} | |
| {{au\_9\_status}} | |
| {{au\_9\_origination}} | |

| AU-9 What is the solution and how is it implemented? |
| --- |
| {{au\_9\_implementation}} |

AU-9 (2) Control Enhancement (M) (H)

The information system backs up audit records [*FedRAMP Assignment: at least weekly*] onto a physically different system or system component than the system or component being audited.

| AU-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_9\_2\_role}} | |
| Parameter AU-09(2): {{au\_9\_2\_parameter}} | |
| {{au\_9\_2\_status}} | |
| {{au\_9\_2\_origination}} | |

| AU-9 (2) What is the solution and how is it implemented? |
| --- |
| {{au\_9\_2\_implementation}} |

AU-9 (3) Control Enhancement (H)

The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

| AU-9 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_9\_3\_role}} | |
| {{au\_9\_3\_status}} | |
| {{au\_9\_3\_origination}} | |

| AU-9 (3) What is the solution and how is it implemented? |
| --- |
| {{au\_9\_3\_implementation}} |

AU-9 (4) Control Enhancement (M) (H)

The organization authorizes access to management of audit functionality to only [*Assignment: organization-defined subset of privileged users*].

| AU-9 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_9\_4\_role}} | |
| Parameter AU-09(4): {{au\_9\_4\_parameter}} | |
| {{au\_9\_4\_status}} | |
| {{au\_9\_4\_origination}} | |

| AU-9 (4) What is the solution and how is it implemented? |
| --- |
| {{au\_9\_4\_implementation}} |

AU-10 Non-repudiation (H)

The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [*FedRAMP Assignment: minimum actions including the addition, modification, deletion, approval, sending, or receiving of data*].

| AU-10 | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_10\_role}} | |
| Parameter AU-10: {{au\_10\_parameter}} | |
| {{au\_10\_status}} | |
| {{au\_10\_origination}} | |

| AU-10 What is the solution and how is it implemented? |
| --- |
| {{au\_10\_implementation}} |

AU-11 Audit Record Retention (H)

The organization retains audit records for [*FedRAMP Assignment: at least one (1) year*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

**AU-11 Additional FedRAMP Requirements and Guidance:**

**Requirement**: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements

| AU-11 | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_11\_role}} | |
| Parameter AU-11: {{au\_11\_parameter}} | |
| {{au\_11\_status}} | |
| {{au\_11\_origination}} | |

| AU-11 What is the solution and how is it implemented? |
| --- |
| {{au\_11\_implementation}} |

AU-12 Audit Generation (L) (M) (H)

The information system:

1. Provides audit record generation capability for the auditable events defined in AU-2 a. at [*FedRAMP Assignment:* *all information system components where audit capability is deployed/available*];
2. Allows [*Assignment: organization-defined personnel or roles*] to select which auditable events are to be audited by specific components of the information system; and
3. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

| AU-12 | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_12\_role}} | |
| Parameter AU-12(a): {{au\_12\_a\_parameter}} | |
| Parameter AU-12(b): {{au\_12\_b\_parameter}} | |
| {{au\_12\_status}} | |
| {{au\_12\_origination}} | |

| AU-12 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{au\_12\_a\_implementation}} |
| **Part b** | {{au\_12\_b\_implementation}} |
| **Part c** | {{au\_12\_c\_implementation}} |

AU-12 (1) Control Enhancement (H)

The information system compiles audit records from [*FedRAMP Assignment: all network, data storage, and computing devices*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail*].

| AU-12 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_12\_1\_role}} | |
| Parameter AU-12 (1)-1: {{au\_12\_1\_1\_parameter}} | |
| Parameter AU-12 (1)-2: {{au\_12\_1\_2\_parameter}} | |
| {{au\_12\_1\_status}} | |
| {{au\_12\_1\_origination}} | |

| AU-12 (1) What is the solution and how is it implemented? |
| --- |
| {{au\_12\_1\_implementation}} |

AU-12 (3) Control Enhancement (H)

The information system provides the capability for [*FedRAMP* *Assignment*: *service provider-defined individuals or roles with audit configuration responsibilities*] to change the auditing to be performed on [*FedRAMP* *Assignment*: *all network, data storage, and computing devices*] based on [*Assignment*: *organization-defined threat situations*] within [*Assignment*: *organization-defined time thresholds*].

| AU-12 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{au\_12\_3\_role}} | |
| Parameter AU-12 (3)-1: {{au\_12\_3\_1\_parameter}} | |
| Parameter AU-12 (3)-2: {{au\_12\_3\_2\_parameter}} | |
| Parameter AU-12 (3)-3: {{au\_12\_3\_3\_parameter}} | |
| Parameter AU-12 (3)-4: {{au\_12\_3\_4\_parameter}} | |
| {{au\_12\_3\_status}} | |
| {{au\_12\_3\_origination}} | |

| AU-12 (3) What is the solution and how is it implemented? |
| --- |
| {{au\_12\_3\_implementation}} |

## Security Assessment and Authorization (CA)

CA-1 Certification, Authorization, Security Assessment Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*FedRAMP Assignment: organization-defined personnel or roles*]
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
2. Reviews and updates the current:
   1. Security assessment and authorization policy [*FedRAMP Assignment: at least annually*] and
   2. Security assessment and authorization procedures [*FedRAMP Assignment: at least at least annually or whenever a significant change occurs*].

| CA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_1\_role}} | |
| Parameter CA-01(a): {{ca\_1\_a\_parameter}} | |
| Parameter CA-01(b)(1): {{ca\_1\_b\_1\_parameter}} | |
| Parameter CA-01(b)(2): {{ca\_1\_b\_2\_parameter}} | |
| {{ca\_1\_status}} | |
| {{ca\_1\_origination}} | |

| CA-1 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ca\_1\_a\_implementation}} |
| **Part b** | {{ca\_1\_b\_implementation}} |

CA-2 Security Assessments (L) (M) (H)

The organization:

1. Develops a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine security control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assesses the security controls in the information system and its environment of operation [*FedRAMP Assignment: at least annually]* determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security control assessment to [*FedRAMP Assignment: individuals or roles to include the FedRAMP Program Management Office (PMO)*].

**CA-2 Additional FedRAMP Requirements and Guidance**

**Guidance:** See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Annual Assessment Guidance

<https://www.FedRAMP.gov/documents/>

| CA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_2\_role}} | |
| Parameter CA-02(b): {{ca\_2\_b\_parameter}} | |
| Parameter CA-02(d): {{ca\_2\_d\_parameter}} | |
| {{ca\_2\_status}} | |
| {{ca\_2\_origination}} | |

| CA-2 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ca\_2\_a\_implementation}} |
| **Part b** | {{ca\_2\_b\_implementation}} |
| **Part c** | {{ca\_2\_c\_implementation}} |
| **Part d** | {{ca\_2\_d\_implementation}} |

CA-2 (1) Control Enhancement (L) (M) (H)

The organization employs assessors or assessment teams with [*FedRAMP Assignment: organization-defined level of independence*] to conduct security control assessments.

**CA-2 (1) Additional FedRAMP Requirements and Guidance:**

**Requirement:** For JAB Authorization, must use an accredited Third-Party Assessment Organization (3PAO).

| CA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_2\_1\_role}} | |
| Parameter CA-02(1): {{ca\_2\_1\_parameter}} | |
| {{ca\_2\_1\_status}} | |
| {{ca\_2\_1\_origination}} | |

| CA-2 (1) What is the solution and how is it implemented? |
| --- |
| {{ca\_2\_1\_implementation}} |

CA-2 (2) Control Enhancement (M) (H)

The organization includes as part of security control assessments, [*FedRAMP Assignment: at least annually*], [*Selection: announced; unannounced*], [*Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing through Red Team exercises; insider threat assessment; performance/load testing;* [*FedRAMP Assignment: organization-defined other forms of security assessment*].

**CA-2 (2) Additional FedRAMP Requirements and Guidance:**

**Requirement**: To include *'announced'*, *'vulnerability scanning’ to occur at least annually*.

| CA-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_2\_2\_role}} | |
| Parameter CA-2(2)-1: {{ca\_2\_2\_1\_parameter}} | |
| Parameter CA-2(2)-2: {{ca\_2\_2\_2\_parameter}} | |
| Parameter CA-2(2)-3: {{ca\_2\_2\_3\_parameter}} | |
| Parameter CA-2(2)-4: {{ca\_2\_2\_4\_parameter}} | |
| {{ca\_2\_2\_status}} | |
| {{ca\_2\_2\_origination}} | |

| CA-2 (2) What is the solution and how is it implemented? |
| --- |
| {{ca\_2\_2\_implementation}} |

CA-2 (3) Control Enhancement (M) (H)

The organization accepts the results of an assessment of [*FedRAMP Assignment: organization-defined information system*] performed by [*FedRAMP Assignment: any FedRAMP Accredited 3PAO*] when the assessment meets [*FedRAMP Assignment: the conditions of the* JAB/AO *in the FedRAMP Repository*].

| CA-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_2\_3\_role}} | |
| Parameter CA-2(3)-1: {{ca\_2\_3\_1\_parameter}} | |
| Parameter CA-2(3)-2: {{ca\_2\_3\_2\_parameter}} | |
| Parameter CA-2(3)-3: {{ca\_2\_3\_3\_parameter}} | |
| {{ca\_2\_3\_status}} | |
| {{ca\_2\_3\_origination}} | |

| CA-2 (3) What is the solution and how is it implemented? |
| --- |
| {{ca\_2\_3\_implementation}} |

CA-3 System Interconnections (L) (M) (H)

The organization:

1. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
2. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
3. Reviews and updates Interconnection Security Agreements [*FedRAMP Assignment: at least annually and on input from FedRAMP*].

*Table 13‑3. CA-3 Authorized Connections*

| Authorized Connections Information System Name | Name of Organization Microsoft System Connects To | Role and Name of Person Who Signed Connection Agreement | Name and Date of Interconnection Agreement |
| --- | --- | --- | --- |
| CorpNet | Microsoft | Core Services Engineering (CSE, formerly MSIT) Sr. Director, Operations Risk Management  Lisa Reshaur | N/A |
| CorpNet is the Microsoft corporate network. CorpNet contains services run on Microsoft’s corporate network, not dedicated to Office 365, such as source code repositories, system documentation repositories, and change ticketing. | | | |
| Cosmos | Microsoft | Group Program Manager, Cosmos  Ryan Waite | N/A |
| Cosmos is a service, not dedicated to Office 365, that stores and reports on Office 365 log data. Office 365 scrubs logs of customer information before sending logs to Cosmos. | | | |
| Azure (including GSGO) | Microsoft | Azure ISSO  Roger Chiou | N/A |
| Azure is a service, not dedicated to Office 365 MT, that provides services for scalable, on-demand computing services. GSGO provides datacenter and network infrastructure, services and security. GSGO is physically and logically segregated from the public network. | | | |
| Akamai | Akamai | Senior Director, Public Sector  David Yoon | Office 365 and Akamai MOU, 10/10/2018 |
| Akamai is a service, not dedicated to Office 365, that provides Global Traffic Management (GTM), and HTTP Content Delivery. This connection is covered via an ISA with Akamai. | | | |

| CA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_3\_role}} | |
| Parameter CA-03(c): {{ca\_3\_c\_parameter}} | |
| {{ca\_3\_status}} | |
| {{ca\_3\_origination}} | |

| CA-3 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ca\_3\_a\_implementation}} |
| **Part b** | {{ca\_3\_b\_implementation}} |
| **Part c** | {{ca\_3\_c\_implementation}} |

CA-3 (3) Control Enhancement (M) (H)

The organization prohibits the direct connection of an [*FedRAMP Assignment: organization-defined unclassified, non-national security system*] to an external network without the use of [*FedRAMP Assignment: boundary protections which meet Trusted Internet Connection (TIC) requirements*].

**CA-3 (3) Additional FedRAMP Requirements and Guidance:**

**Guidance:** Refer to Appendix H – Cloud Considerations of the TIC Reference Architecture document. Link: <https://www.dhs.gov/publication/tic-reference-architecture-22>

| CA-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_3\_3\_role}} | |
| Parameter CA-3(3)-1: {{ca\_3\_3\_1\_parameter}} | |
| Parameter CA-3(3)-2: {{ca\_3\_3\_2\_parameter}} | |
| {{ca\_3\_3\_status}} | |
| {{ca\_3\_3\_origination}} | |

| CA-3 (3) What is the solution and how is it implemented? |
| --- |
| {{ca\_3\_3\_implementation}} |

CA-3 (5) Control Enhancement (H)

The organization employs [*FedRAMP Selection: deny-all, permit by exception*] policy for allowing [*FedRAMP Assignment: any systems*]to connect to external information systems.

**CA-3 (5) Additional FedRAMP Requirements and Guidance:**

**Guidance**: For JAB Authorization, CSPs shall include details of this control in their architecture briefing.

| CA-3 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_3\_5\_role}} | |
| Parameter CA-3(5)-1: {{ca\_3\_5\_1\_parameter}} | |
| Parameter CA-3(5)-2: {{ca\_3\_5\_2\_parameter}} | |
| {{ca\_3\_5\_status}} | |
| {{ca\_3\_5\_origination}} | |

| CA-3 (5) What is the solution and how is it implemented? |
| --- |
| {{ca\_3\_5\_implementation}} |

CA-5 Plan of Action and Milestones (L) (M) (H)

The organization:

1. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
2. Updates existing plan of action and milestones [*FedRAMP Assignment: at least monthly*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

**CA-5 Additional FedRAMP Requirements and Guidance:**

**Requirement**: Plan of Action & Milestones (POA&M must be provided at least monthly.

**Guidance**: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Plan of Action and Milestones (POA&M) Template Completion Guide

<https://www.fedramp.gov/documents/>

| CA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_5\_role}} | |
| Parameter CA-05(b): {{ca\_5\_b\_parameter}} | |
| {{ca\_5\_status}} | |
| {{ca\_5\_origination}} | |

| CA-5 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ca\_5\_a\_implementation}} |
| **Part b** | {{ca\_5\_b\_implementation}} |

CA-6 Security Authorization (L) (M) (H)

The organization:

1. Assigns a senior-level executive or manager as the authorizing official for the information system;
2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
3. Updates the security authorization [*FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs*].

**CA-6c Additional FedRAMP Requirements and Guidance:**

**Guidance**: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F ([SP 800-37](http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf)). The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO.

| CA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_6\_role}} | |
| Parameter CA-06(c): {{ca\_6\_c\_parameter}} | |
| {{ca\_6\_status}} | |
| {{ca\_6\_origination}} | |

| CA-6 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ca\_6\_a\_implementation}} |
| **Part b** | {{ca\_6\_b\_implementation}} |
| **Part c** | {{ca\_6\_c\_implementation}} |

CA-7 Continuous Monitoring (L) (M) (H)

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Establishment of [*Assignment: organization-defined metrics*] to be monitored;
2. Establishment of [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessments supporting such monitoring;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of organization and the information system to [*FedRAMP Assignment: to meet Federal and FedRAMP requirements*] [*Assignment: organization-defined frequency*].

**CA-7 Additional FedRAMP Requirements and Guidance**:

**Requirement:** Operating System Scans: at least monthly Database and Web Application Scans: at least monthly. All scans performed by Independent Assessor: at least annually.

**Guidance**: CSPs must provide evidence of closure and remediation of a high vulnerability within the timeframe for standard POA&M updates.

**Guidance**: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Continuous Monitoring Strategy Guide

| CA-7 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_7\_role}} | |
| Parameter CA-07(a): {{ca\_7\_a\_parameter}} | |
| Parameter CA-7(b)-1: {{ca\_7\_b\_1\_parameter}} | |
| Parameter CA-7(b)-2: {{ca\_7\_b\_2\_parameter}} | |
| Parameter CA-7(g)-1: {{ca\_7\_g\_1\_parameter}} | |
| Parameter CA-7(g)-2: {{ca\_7\_g\_2\_parameter}} | |
| {{ca\_7\_status}} | |
| {{ca\_7\_origination}} | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ca\_7\_a\_implementation}} |
| **Part b** | {{ca\_7\_b\_implementation}} |
| **Part c** | {{ca\_7\_c\_implementation}} |
| **Part d** | {{ca\_7\_d\_implementation}} |
| **Part e** | {{ca\_7\_e\_implementation}} |
| **Part f** | {{ca\_7\_f\_implementation}} |
| **Part g** | {{ca\_7\_g\_implementation}} |

**CA-7 Additional FedRAMP Requirements and Guidance:**

**Requirement 1:** Operating System Scans: at least monthly

**Requirement 2:** Database and Web Application Scans: at least monthly

**Requirement 3:** All scans performed by Independent Assessor: at least annually

| CA-7 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_7\_r\_role}} | |
| {{ca\_7\_r\_status}} | |
| {{ca\_7\_r\_origination}} | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| **Req. 1** | {{ca\_7\_r\_1\_implementation}} |
| **Req. 2** | {{ca\_7\_r\_2\_implementation}} |
| **Req. 3** | {{ca\_7\_r\_3\_implementation}} |

CA-7 (1) Control Enhancement (M) (H)

The organization employs assessors or assessment teams with [*Assignment: organization-defined level of independence*] to monitor the security controls in the information system on an ongoing basis.

| CA-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_7\_1\_role}} | |
| Parameter CA-7(1): {{ca\_7\_1\_parameter}} | |
| {{ca\_7\_1\_status}} | |
| {{ca\_7\_1\_origination}} | |

| CA-7 (1) What is the solution and how is it implemented? |
| --- |
| {{ca\_7\_1\_implementation}} |

CA-7 (3) Control Enhancement (H)

The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

| CA-7 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_7\_3\_role}} | |
| {{ca\_7\_3\_status}} | |
| {{ca\_7\_3\_origination}} | |

| CA-7 (3) What is the solution and how is it implemented? |
| --- |
| {{ca\_7\_3\_implementation}} |

CA-8 Penetration Testing (M) (H)

The organization conducts penetration testing [*FedRAMP Assignment: at least annually*] on [*Assignment: organization-defined information systems or system components*].

**CA-8 Additional FedRAMP Requirements and Guidance**

**Guidance:** See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Penetration Test Guidance

| CA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_8\_role}} | |
| Parameter CA-8-1: {{ca\_8\_1\_parameter}} | |
| Parameter CA-8-2: {{ca\_8\_2\_parameter}} | |
| {{ca\_8\_status}} | |
| {{ca\_8\_origination}} | |

| CA-8 What is the solution and how is it implemented? |
| --- |
| {{ca\_8\_implementation}} |

CA-8 (1) Control Enhancement (M) (H)

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

| CA-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_8\_1\_role}} | |
| {{ca\_8\_1\_status}} | |
| {{ca\_8\_1\_origination}} | |

| CA-8 (1) What is the solution and how is it implemented? |
| --- |
| {{ca\_8\_1\_implementation}} |

CA-9 Internal System Connections (L) (M) (H)

The organization:

1. Authorizes internal connections of [*Assignment: organization-defined information system components or classes of components*] to the information system; and
2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

| CA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ca\_9\_role}} | |
| Parameter CA-9(a): {{ca\_9\_a\_parameter}} | |
| {{ca\_9\_status}} | |
| {{ca\_9\_origination}} | |

| CA-9 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{ca\_9\_a\_implementation}} |
| **Part b** | {{ca\_9\_b\_implementation}} |

## Configuration Management (CM)

CM-1 Configuration Management Policies and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*].
   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
2. Reviews and updates the current:
   1. Configuration management policy [*FedRAMP Assignment: at least annually]*; and
   2. Configuration management procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| CM-1 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_1\_role}} | |
| Parameter CM-01(a): {{cm\_1\_a\_parameter}} | |
| Parameter CM-01(b)(1): {{cm\_1\_b\_1\_parameter}} | |
| Parameter CM-01(b)(2): {{cm\_1\_b\_2\_parameter}} | |
| {{cm\_1\_status}} | |
| {{cm\_1\_origination}} | |

| CM-1 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_1\_a\_implementation}} |
| **Part b** | {{cm\_1\_b\_implementation}} |

CM-2 Baseline Configuration (L) (M) (H)

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

| CM-2 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_2\_role}} | |
| {{cm\_2\_status}} | |
| {{cm\_2\_origination}} | |

| CM-2 What is the solution and how is it implemented? |
| --- |
| {{cm\_2\_implementation}} |

CM-2 (1) Control Enhancement (H)

The organization reviews and updates the baseline configuration of the information system:

1. [*FedRAMP Assignment: at least annually or when a significant change occurs*];
2. When required due to [*FedRAMP Assignment: to include when directed by the JAB*]; and
3. As an integral part of information system component installations and upgrades.

**CM-2 (1) (a) Additional FedRAMP Requirements and Guidance:**

**Guidance**: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F, Page F-7.

| CM-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_2\_1\_role}} | |
| Parameter CM-02(1)(a): {{cm\_2\_1\_a\_parameter}} | |
| Parameter CM-02(1)(b): {{cm\_2\_1\_b\_parameter}} | |
| {{cm\_2\_1\_status}} | |
| {{cm\_2\_1\_origination}} | |

| CM-2 (1) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_2\_1\_a\_implementation}} |
| **Part b** | {{cm\_2\_1\_b\_implementation}} |
| **Part c** | {{cm\_2\_1\_c\_implementation}} |

CM-2 (2) Control Enhancement (M) (H)

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

| CM-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_2\_2\_role}} | |
| {{cm\_2\_2\_status}} | |
| {{cm\_2\_2\_origination}} | |

| CM-2 (2) What is the solution and how is it implemented? |
| --- |
| {{cm\_2\_2\_implementation}} |

CM-2 (3) Control Enhancement (H)

The organization retains [*FedRAMP Assignment: the previously approved baseline configuration of IS components* ] to support rollback.

| CM-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_2\_3\_role}} | |
| Parameter CM-02(3): {{cm\_2\_3\_parameter}} | |
| {{cm\_2\_3\_status}} | |
| {{cm\_2\_3\_origination}} | |

| CM-2 (3) What is the solution and how is it implemented? |
| --- |
| {{cm\_2\_3\_implementation}} |

CM-2 (7) Control Enhancement (M) (H)

The organization:

1. Issues [*Assignment: organization-defined information systems, system components, or devices*] with [*Assignment: organization-defined configurations*] to individuals traveling to locations that the organization deems to be of significant risk; and
2. Applies [*Assignment: organization-defined security safeguards*] to the devices when the individuals return.

| CM-2 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_2\_7\_role}} | |
| Parameter CM-2(7)(a)-1: {{cm\_2\_7\_a\_1\_parameter}} | |
| Parameter CM-2(7)(a)-2: {{cm\_2\_7\_a\_2\_parameter}} | |
| Parameter CM-2(7)(b): {{cm\_2\_7\_b\_parameter}} | |
| {{cm\_2\_7\_status}} | |
| {{cm\_2\_7\_origination}} | |

| CM-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_2\_7\_a\_implementation}} |
| **Part b** | {{cm\_2\_7\_b\_implementation}} |

CM-3 Configuration Change Control (M) (H)

The organization:

1. Determines the types of changes to the information system that are configuration-controlled;
2. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
3. Documents configuration change decisions associated with the information system;
4. Implements approved configuration-controlled changes to the information system;
5. Retains records of configuration-controlled changes to the information system for [*Assignment: organization-defined time period*];

**CM-3 (e) Additional FedRAMP Requirements and Guidance**:

**Guidance**: In accordance with record retention policies and procedures.

1. Audits and reviews activities associated with configuration-controlled changes to the information system; and
2. Coordinates and provides oversight for configuration change control activities through [*FedRAMP Assignment: see additional FedRAMP requirements and guidance*] that convenes [*Selection (one or more): [Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*].

**CM-3 Additional FedRAMP Requirements and Guidance:**

**Requirement**: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the JAB/AO.

| CM-3 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_3\_role}} | |
| Parameter CM-3(e): {{cm\_3\_e\_parameter}} | |
| Parameter CM-3(g)-1: {{cm\_3\_g\_1\_parameter}} | |
| Parameter CM-3(g)-2: {{cm\_3\_g\_2\_parameter}} | |
| Parameter CM-3(g)-3: {{cm\_3\_g\_3\_parameter}} | |
| {{cm\_3\_status}} | |
| {{cm\_3\_origination}} | |

| CM-3 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_3\_a\_implementation}} |
| **Part b** | {{cm\_3\_b\_implementation}} |
| **Part c** | {{cm\_3\_c\_implementation}} |
| **Part d** | {{cm\_3\_d\_implementation}} |
| **Part e** | {{cm\_3\_e\_implementation}} |
| **Part f** | {{cm\_3\_f\_implementation}} |
| **Part g** | {{cm\_3\_g\_implementation}} |

CM-3 (1) Control Enhancement (H)

The organization employs automated mechanisms to:

1. Document proposed changes to the information system;
2. Notify [*Assignment: organization-defined configuration management approval authorities*] of proposed changes to the information system and request change approval;
3. Highlight proposed changes to the information system that have not been approved or disapproved by [*FedRAMP Assignment: organization agreed upon time period*];
4. Prohibit changes to the information system until designated approvals are received;
5. Document all changes to the information system; and
6. Notify [*FedRAMP Assignment: organization-defined configuration management approval authorities*] when approved changes to the information system are completed.

| CM-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_3\_1\_role}} | |
| Parameter CM-3 (1)(b): {{cm\_3\_1\_b\_parameter}} | |
| Parameter CM-3 (1)(c): {{cm\_3\_1\_c\_parameter}} | |
| Parameter CM-3 (1)(f): {{cm\_3\_1\_f\_parameter}} | |
| {{cm\_3\_1\_status}} | |
| {{cm\_3\_1\_origination}} | |

| CM-3 (1) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_3\_1\_a\_implementation}} |
| **Part b** | {{cm\_3\_1\_b\_implementation}} |
| **Part c** | {{cm\_3\_1\_c\_implementation}} |
| **Part d** | {{cm\_3\_1\_d\_implementation}} |
| **Part e** | {{cm\_3\_1\_e\_implementation}} |
| **Part f** | {{cm\_3\_1\_f\_implementation}} |

CM-3 (2) Control Enhancement (M)(H)

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

| CM-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_3\_2\_role}} | |
| {{cm\_3\_2\_status}} | |
| {{cm\_3\_2\_origination}} | |

| CM-3 (2) What is the solution and how is it implemented? |
| --- |
| {{cm\_3\_2\_implementation}} |

CM-3 (4) Enhancement (H)

The organization requires an information security representative to be a member of the [*FedRAMP Assignment: configuration control board (CCB) or similar (as defined in CM-3)*].

| CM-3 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_3\_4\_role}} | |
| Parameter CM-3 (4): {{cm\_3\_4\_parameter}} | |
| {{cm\_3\_4\_status}} | |
| {{cm\_3\_4\_origination}} | |

| CM-3 (4) What is the solution and how is it implemented? |
| --- |
| {{cm\_3\_4\_implementation}} |

CM-3 (6) Enhancement (H)

The organization ensures that cryptographic mechanisms used to provide [*FedRAMP Assignment: all security safeguards that rely on cryptography*] are under configuration management.

| CM-3 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_3\_6\_role}} | |
| Parameter CM-3 (6): {{cm\_3\_6\_parameter}} | |
| {{cm\_3\_6\_status}} | |
| {{cm\_3\_6\_origination}} | |

| CM-3 (6) What is the solution and how is it implemented? |
| --- |
| {{cm\_3\_6\_implementation}} |

CM-4 Security Impact Analysis (L) (M) (H)

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

| CM-4 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_4\_role}} | |
| {{cm\_4\_status}} | |
| {{cm\_4\_origination}} | |

| CM-4 What is the solution and how is it implemented? |
| --- |
| {{cm\_4\_implementation}} |

CM-4 (1) Control Enhancement (H)

The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

| CM-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_4\_1\_role}} | |
| {{cm\_4\_1\_status}} | |
| {{cm\_4\_1\_origination}} | |

| CM-4 (1) What is the solution and how is it implemented? |
| --- |
| {{cm\_4\_1\_implementation}} |

CM-5 Access Restrictions for Change (M) (H)

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

| CM-5 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_5\_role}} | |
| {{cm\_5\_status}} | |
| {{cm\_5\_origination}} | |

| CM-5 What is the solution and how is it implemented? |
| --- |
| {{cm\_5\_implementation}} |

CM-5 (1) Control Enhancement (M) (H)

The information system enforces access restrictions and supports auditing of the enforcement actions.

| CM-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_5\_1\_role}} | |
| {{cm\_5\_1\_status}} | |
| {{cm\_5\_1\_origination}} | |

| CM-5 (1) What is the solution and how is it implemented? |
| --- |
| **{**{cm\_5\_1\_implementation}} |

CM-5 (2) Control Enhancement (H)

The organization reviews information system changes [*FedRAMP* *Assignment: at least every thirty (30) days*] and [*Assignment: organization-defined circumstances*] to determine whether unauthorized changes have occurred.

| CM-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_5\_2\_role}} | |
| Parameter CM-5 (2)-1: {{cm\_5\_2\_1\_parameter}} | |
| Parameter CM-5 (2)-2: {{cm\_5\_2\_2\_parameter}} | |
| {{cm\_5\_2\_status}} | |
| {{cm\_5\_2\_origination}} | |

| CM-5 (2) What is the solution and how is it implemented? |
| --- |
| {{cm\_5\_2\_implementation}} |

CM-5 (3) Control Enhancement (M) (H)

The information system prevents the installation of [*Assignment: organization-defined software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

**CM-5 (3) Additional FedRAMP Requirements and Guidance**:

**Guidance**: If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be used.

| CM-5 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_5\_3\_role}} | |
| Parameter CM-05(3): {{cm\_5\_3\_parameter}} | |
| {{cm\_5\_3\_status}} | |
| {{cm\_5\_3\_origination}} | |

| CM-5 (3) What is the solution and how is it implemented? |
| --- |
| {{cm\_5\_3\_implementation}} |

CM-5 (5) Control Enhancement (M) (H)

The organization:

1. Limits privileges to change information system components and system-related information within a production or operational environment; and
2. Reviews and reevaluates privileges [*FedRAMP Assignment: at least quarterly*].

| CM-5 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_5\_5\_role}} | |
| Parameter CM-05(5)(b): {{cm\_5\_5\_b\_parameter}} | |
| {{cm\_5\_5\_status}} | |
| {{cm\_5\_5\_origination}} | |

| CM-5 (5) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_5\_5\_a\_implementation}} |
| **Part b** | {{cm\_5\_5\_b\_implementation}} |

CM-6 Configuration Settings (L) (M) (H)

The organization:

1. Establishes and documents configuration settings for information technology products employed within the information system using [*FedRAMP Assignment: see CM-6(a) Additional FedRAMP Requirements and Guidance*] that reflect the most restrictive mode consistent with operational requirements;

**CM-6(a) Additional FedRAMP Requirements and Guidance:**

**Requirement 1:** The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

**Requirement 2:** The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) (<http://scap.nist.gov/>) validated or SCAP compatible (if validated checklists are not available).

**Guidance:** Information on the USGCB checklists can be found at: <https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline>.

1. Implements the configuration settings;
2. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components* based on [*Assignment: organization-defined operational requirements*]; and
3. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

| CM-6 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_6\_role}} | |
| Parameter CM-6(a)-1: {{cm\_6\_a\_1\_parameter}} | |
| Parameter CM-6(a)-2: {{cm\_6\_a\_2\_parameter}} | |
| Parameter CM-6(c)-1: {{cm\_6\_c\_1\_parameter}} | |
| Parameter CM-6(c)-2: {{cm\_6\_c\_2\_parameter}} | |
| {{cm\_6\_status}} | |
| {{cm\_6\_origination}} | |

| CM-6 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_6\_a\_implementation}} |
| **Part b** | {{cm\_6\_b\_implementation}} |
| **Part c** | {{cm\_6\_c\_implementation}} |
| **Part d** | {{cm\_6\_d\_implementation}} |

CM-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*Assignment: organization-defined information system components*].

| CM-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_6\_1\_role}} | |
| Parameter CM-06(1): {{cm\_6\_1\_parameter}} | |
| {{cm\_6\_1\_status}} | |
| {{cm\_6\_1\_origination}} | |

| CM-6 (1) What is the solution and how is it implemented? |
| --- |
| {{cm\_6\_1\_implementation}} |

CM-6 (2) Control Enhancement (H)

The organization employs [*Assignment: organization-defined security safeguards*] to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].

| CM-6 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_6\_2\_role}} | |
| Parameter CM-6 (2)-1: {{cm\_6\_2\_1\_parameter}} | |
| Parameter CM-6 (2)-2: {{cm\_6\_2\_2\_parameter}} | |
| {{cm\_6\_2\_status}} | |
| {{cm\_6\_2\_origination}} | |

| CM-6 (2) What is the solution and how is it implemented? |
| --- |
| {{cm\_6\_2\_implementation}} |

CM-7 Least Functionality (L) (M) (H)

The organization:

1. Configures the information system to provide only essential capabilities; and
2. Prohibits or restricts the use of the following functions, ports, protocols, and/or services [*FedRAMP Assignment: United States Government Configuration Baseline (USGCB)]*

**CM-7 Additional FedRAMP Requirements and Guidance:**

**Requirement**: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

**Guidance**: Information on the USGCB checklists can be found at: <https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline>

Partially derived from AC-17 (8).

| CM-7 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_7\_role}} | |
| Parameter CM-07(b): {{cm\_7\_parameter}} | |
| {{cm\_7\_status}} | |
| {{cm\_7\_origination}} | |

| CM-7 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_7\_a\_implementation}} |
| **Part b** | {{cm\_7\_b\_implementation}} |

CM-7 (1) Control Enhancement (M) (H)

The organization:

1. Reviews the information system [*FedRAMP Assignment: at least monthly*] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
2. Disables [*Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure*].

| CM-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_7\_1\_role}} | |
| Parameter CM-07(1)(a): {{cm\_7\_1\_a\_parameter}} | |
| Parameter CM-07(1)(b): {{cm\_7\_1\_b\_parameter}} | |
| {{cm\_7\_1\_status}} | |
| {{cm\_7\_1\_origination}} | |

| CM-7 (1) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_7\_1\_a\_implementation}} |
| **Part b** | {{cm\_7\_1\_b\_implementation}} |

CM-7 (2) Control Enhancement (M) (H)

The information system prevents program execution in accordance with [*Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage*].

**CM-7(2) Additional FedRAMP Requirements and Guidance**:

**Guidance**: This control shall be implemented in a technical manner on the information system to only allow programs to run that adhere to the policy (i.e., white listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run.

| CM-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_7\_2\_role}} | |
| Parameter CM-07(2): {{cm\_7\_2\_parameter}} | |
| {{cm\_7\_2\_status}} | |
| {{cm\_7\_2\_origination}} | |

| CM-7 (2) What is the solution and how is it implemented? |
| --- |
| {{cm\_7\_2\_implementation}} |

CM-7 (5) Control Enhancement (H)

The organization:

1. Identifies [*Assignment: organization-defined software programs authorized to execute on the information system*];
2. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and
3. Reviews and updates the list of authorized software programs [*FedRAMP Assignment: at least quarterly or when there is a change]*.

| CM-7 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_7\_5\_role}} | |
| Parameter CM-07(5)(a): {{cm\_7\_5\_a\_parameter}} | |
| Parameter CM-07(5)(c): {{cm\_7\_5\_c\_parameter}} | |
| {{cm\_7\_5\_status}} | |
| {{cm\_7\_5\_origination}} | |

| CM-7 (5) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_7\_5\_a\_implementation}} |
| **Part b** | {{cm\_7\_5\_b\_implementation}} |
| **Part c** | {{cm\_7\_5\_c\_implementation}} |

CM-8 Information System Component Inventory (L) (M) (H)

The organization:

1. Develops and documents an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Includes all components within the authorization boundary of the information system;
   3. Is at the level of granularity deemed necessary for tracking and reporting; and
   4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]*; and
2. Reviews and updates the information system component inventory [*FedRAMP Assignment: at least monthly]*.

**CM-8 Additional FedRAMP Requirements and Guidance**:

**Requirement**: Must be provided at least monthly or when there is a change.

| CM-8 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_8\_role}} | |
| Parameter CM-08(a)(4): {{cm\_8\_a\_4\_parameter}} | |
| Parameter CM-08(b): {{cm\_8\_b\_parameter}} | |
| {{cm\_8\_status}} | |
| {{cm\_8\_origination}} | |

| CM-8 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_8\_a\_implementation}} |
| **Part b** | {{cm\_8\_b\_implementation}} |

CM-8 (1) Control Enhancement (M) (H)

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

| CM-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_8\_1\_role}} | |
| {{cm\_8\_1\_status}} | |
| {{cm\_8\_1\_origination}} | |

| CM-8 (1) What is the solution and how is it implemented? |
| --- |
| {{cm\_8\_1\_implementation}} |

CM-8 (2) Control Enhancement (H)

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

| CM-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_8\_2\_role}} | |
| {{cm\_8\_2\_status}} | |
| {{cm\_8\_2\_origination}} | |

| CM-8 (2) What is the solution and how is it implemented? |
| --- |
| {{cm\_8\_2\_implementation}} |

CM-8 (3) Control Enhancement (M) (H)

The organization:

1. Employs automated mechanisms [*FedRAMP Assignment: Continuously, using automated mechanisms with a maximum five-minute delay in detection*] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
2. Takes the following actions when unauthorized components are detected: [*Selection (one or more): disables network access by such components; isolates the components; notifies* [*Assignment: organization-defined personnel or roles*].

| CM-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_8\_3\_role}} | |
| Parameter CM-08(3)(a): {{cm\_8\_3\_a\_parameter}} | |
| Parameter CM-08(3)(b): {{cm\_8\_3\_b\_parameter}} | |
| {{cm\_8\_3\_status}} | |
| {{cm\_8\_3\_origination}} | |

| CM-8 (3) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_8\_3\_a\_implementation}} |
| **Part b** | {{cm\_8\_3\_b\_implementation}} |

CM-8 (4) Control Enhancement (H)

The organization includes in the information system component inventory information, a means for identifying by [*Selection (one or more): name;* [*FedRAMP Assignment: position and role*]], individuals responsible/accountable for administering those components.

| CM-8 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_8\_4\_role}} | |
| Parameter CM-8 (4): {{cm\_8\_4\_parameter}} | |
| {{cm\_8\_4\_status}} | |
| {{cm\_8\_4\_origination}} | |

| CM-8 (4) What is the solution and how is it implemented? |
| --- |
| {{cm\_8\_4\_implementation}} |

CM-8 (5) Control Enhancement (M) (H)

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

| CM-8 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_8\_5\_role}} | |
| {{cm\_8\_5\_status}} | |
| {{cm\_8\_5\_origination}} | |

| CM-8 (5) What is the solution and how is it implemented? |
| --- |
| {{cm\_8\_5\_implementation}} |

CM-9 Configuration Management Plan (M) (H)

The organization develops, documents, and implements a configuration management plan for the information system that:

1. Addresses roles, responsibilities, and configuration management processes and procedures;
2. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
3. Defines the configuration items for the information system and places the configuration items under configuration management; and
4. Protects the configuration management plan for unauthorized disclosure and modification.

| CM-9 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_9\_role}} | |
| {{cm\_9\_status}} | |
| {{cm\_9\_origination}} | |

| CM-9 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_9\_a\_implementation}} |
| **Part b** | {{cm\_9\_b\_implementation}} |
| **Part c** | {{cm\_9\_c\_implementation}} |
| **Part d** | {{cm\_9\_d\_implementation}} |

CM-10 Software Usage Restrictions (L) (M) (H)

The organization:

1. Uses software and associated documentation in accordance with contract agreements and copyright laws;
2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
3. Controls and documents 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: {{cm\_10\_role}} | |
| {{cm\_10\_status}} | |
| {{cm\_10\_origination}} | |

| CM-10 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_10\_a\_implementation}} |
| **Part b** | {{cm\_10\_b\_implementation}} |
| **Part c** | {{cm\_10\_c\_implementation}} |

CM-10 (1) Control Enhancement (M) (H)

The organization establishes the following restrictions on the use of open source software: [*Assignment: organization-defined restrictions*].

| CM-10 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_10\_1\_role}} | |
| Parameter CM-10(1): {{cm\_10\_1\_parameter}} | |
| {{cm\_10\_1\_status}} | |
| {{cm\_10\_1\_origination}} | |

| CM-10 (1) What is the solution and how is it implemented? |
| --- |
| {{cm\_10\_1\_implementation}} |

CM-11 User-Installed Software (M) (H)

The organization:

1. Establishes [*Assignment: organization-defined policies*] governing the installation of software by users;
2. Enforces software installation policies through [*Assignment: organization-defined methods*]; and
3. Monitors policy compliance [*FedRAMP* *Assignment: Continuously (via CM-7 (5))*].

| CM-11 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_11\_role}} | |
| Parameter CM-11(a): {{cm\_11\_a\_parameter}} | |
| Parameter CM-11(b): {{cm\_11\_b\_parameter}} | |
| Parameter CM-11(c): {{cm\_11\_c\_parameter}} | |
| {{cm\_11\_status}} | |
| {{cm\_11\_origination}} | |

| CM-11 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cm\_11\_a\_implementation}} |
| **Part b** | {{cm\_11\_b\_implementation}} |
| **Part c** | {{cm\_11\_c\_implementation}} |

CM-11 (1) Control Enhancement (H)

The information system alerts [*Assignment: organization-defined personnel or roles*] when the unauthorized installation of software is detected.

| CM-11 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cm\_11\_1\_role}} | |
| Parameter CM-11 (1): {{cm\_11\_1\_parameter}} | |
| {{cm\_11\_1\_status}} | |
| {{cm\_11\_1\_origination}} | |

| CM-11 (1) What is the solution and how is it implemented? |
| --- |
| {{cm\_11\_1\_implementation}} |

## Contingency Planning (CP)

CP-1 Contingency Planning Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]*:
   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
2. Reviews and updates the current:
   1. Contingency planning policy [*FedRAMP Assignment: at least annually*]; and
   2. Contingency planning procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| CP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_1\_role}} | |
| Parameter CP-01(a)(1): {{cp\_1\_a\_1\_parameter}} | |
| Parameter CP-01(a)(2): {{cp\_1\_a\_2\_parameter}} | |
| Parameter CP-01(b)(1): {{cp\_1\_b\_1\_parameter}} | |
| Parameter CP-01(b)(2): {{cp\_1\_b\_2\_parameter}} | |
| {{cp\_1\_status}} | |
| {{cp\_1\_origination}} | |

| CP-1 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cp\_1\_a\_implementation}} |
| **Part b** | {{cp\_1\_b\_implementation}} |

CP-2 Contingency Plan (L) (M) (H)

The organization:

1. Develops a contingency plan for the information system that:
   1. Identifies essential missions 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 missions and business functions despite an information system disruption, compromise, or failure;
   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
   6. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];
2. Distributes copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];
3. Coordinates contingency planning activities with incident handling activities;
4. Reviews the contingency plan for the information system [*FedRAMP Assignment: at least annually*];
5. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
6. Communicates contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*]; and
7. Protects the contingency plan from unauthorized disclosure and modification.

**CP-2 Additional FedRAMP Requirements and Guidance:**

**Requirement**: For JAB authorizations the contingency lists include designated FedRAMP personnel.

| CP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_2\_role}} | |
| Parameter CP-02(a)(6): {{cp\_2\_a\_6\_parameter}} | |
| Parameter CP-02(b): {{cp\_2\_b\_parameter}} | |
| Parameter CP-02(d): {{cp\_2\_d\_parameter}} | |
| Parameter CP-02(f): {{cp\_2\_f\_parameter}} | |
| {{cp\_2\_status}} | |
| {{cp\_2\_origination}} | |

| CP-2 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cp\_2\_a\_implementation}} |
| **Part b** | {{cp\_2\_b\_implementation}} |
| **Part c** | {{cp\_2\_c\_implementation}} |
| **Part d** | {{cp\_2\_d\_implementation}} |
| **Part e** | {{cp\_2\_e\_implementation}} |
| **Part f** | {{cp\_2\_f\_implementation}} |
| **Part g** | {{cp\_2\_g\_implementation}} |

CP-2 (1) Control Enhancement (M) (H)

The organization coordinates contingency plan development with organizational elements responsible for related plans.

| CP-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_2\_1\_role}} | |
| {{cp\_2\_1\_status}} | |
| {{cp\_2\_1\_origination}} | |

| CP-2 (1) What is the solution and how is it implemented? |
| --- |
| {{cp\_2\_1\_implementation}} |

CP-2 (2) Control Enhancement (M) (H)

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

| CP-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_2\_2\_role}} | |
| {{cp\_2\_2\_status}} | |
| {{cp\_2\_2\_origination}} | |

| CP-2 (2) What is the solution and how is it implemented? |
| --- |
| {{cp\_2\_2\_implementation}} |

CP-2 (3) Control Enhancement (M) (H)

The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*], of contingency plan activation.

| CP-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_2\_3\_role}} | |
| Parameter CP-02(3): {{cp\_2\_3\_parameter}} | |
| {{cp\_2\_3\_status}} | |
| {{cp\_2\_3\_origination}} | |

| CP-2 (3) What is the solution and how is it implemented? |
| --- |
| {{cp\_2\_3\_implementation}} |

CP-2 (4) Control Enhancement (H)

The organization plans for the resumption of all missions and business functions within [*FedRAMP* *Assignment: time period defined in service provider and organization Service Level Agreement (SLA)*] of contingency plan activation.

| CP-2 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_2\_4\_role}} | |
| Parameter CP-2 (4): {{cp\_2\_4\_parameter}} | |
| {{cp\_2\_4\_status}} | |
| {{cp\_2\_4\_origination}} | |

| CP-2 (4) What is the solution and how is it implemented? |
| --- |
| {{cp\_2\_4\_implementation}} |

CP-2 (5) Control Enhancement (H)

The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

| CP-2 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_2\_5\_role}} | |
| {{cp\_2\_5\_status}} | |
| {{cp\_2\_5\_origination}} | |

| CP-2 (5) What is the solution and how is it implemented? |
| --- |
| {{cp\_2\_5\_implementation}} |

CP-2 (8) Control Enhancement (M) (H)

The organization identifies critical information system assets supporting essential missions and business functions.

| CP-2 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_2\_8\_role}} | |
| {{cp\_2\_8\_status}} | |
| {{cp\_2\_8\_origination}} | |

| CP-2 (8) What is the solution and how is it implemented? |
| --- |
| {{cp\_2\_8\_implementation}} |

CP-3 Contingency Training (L) (M) (H)

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

1. Within [*FedRAMP Assignment: ten (10) days*] of assuming a contingency role or responsibility;
2. When required by information system changes; and
3. [*FedRAMP Assignment: at least annually*] thereafter.

| CP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_3\_role}} | |
| Parameter CP-03(a): {{cp\_3\_a\_parameter}} | |
| Parameter CP-03(c): {{cp\_3\_c\_parameter}} | |
| {{cp\_3\_status}} | |
| {{cp\_3\_origination}} | |

| CP-3 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cp\_3\_a\_implementation}} |
| **Part b** | {{cp\_3\_b\_implementation}} |
| **Part c** | {{cp\_3\_c\_implementation}} |

CP-3 (1) Control Enhancement (H)

The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

| CP-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_3\_1\_role}} | |
| {{cp\_3\_1\_status}} | |
| {{cp\_3\_1\_origination}} | |

| CP-3 (1) What is the solution and how is it implemented? |
| --- |
| {{cp\_3\_1\_implementation}} |

CP-4 Contingency Plan Testing (H)

The organization:

1. Tests the contingency plan for the information system [*FedRAMP Assignment: at least annually*] using [*FedRAMP Assignment: functional exercises*] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

**CP-4(a) Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. Test plans are approved and accepted by the JAB/AO prior to initiating testing.

1. Reviews the contingency plan test results; and
2. Initiates corrective actions, if needed.

| CP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_4\_role}} | |
| Parameter CP-4(a)-1: {{cp\_4\_a\_1\_parameter}} | |
| Parameter CP-4(a)-2: {{cp\_4\_a\_2\_parameter}} | |
| {{cp\_4\_status}} | |
| {{cp\_4\_origination}} | |

| CP-4 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cp\_4\_a\_implementation}} |
| **Part b** | {{cp\_4\_b\_implementation}} |
| **Part c** | {{cp\_4\_c\_implementation}} |

CP-4 (1) Control Enhancement (M) (H)

The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

| CP-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_4\_1\_role}} | |
| {{cp\_4\_1\_status}} | |
| {{cp\_4\_1\_origination}} | |

| CP-4 (1) What is the solution and how is it implemented? |
| --- |
| {{cp\_4\_1\_implementation}} |

CP-4 (2) Control Enhancement (H)

The organization tests the contingency plan at the alternate processing site:

1. To familiarize contingency personnel with the facility and available resources; and
2. To evaluate the capabilities of the alternate processing site to support contingency operations.

| CP-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_4\_2\_role}} | |
| {{cp\_4\_2\_status}} | |
| {{cp\_4\_2\_origination}} | |

| CP-4 (2) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cp\_4\_2\_a\_implementation}} |
| **Part b** | {{cp\_4\_2\_b\_implementation}} |

CP-6 Alternate Storage Site (M) (H)

The organization:

1. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
2. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

| CP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_6\_role}} | |
| {{cp\_6\_status}} | |
| {{cp\_6\_origination}} | |

| CP-6 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cp\_6\_a\_implementation}} |
| **Part b** | {{cp\_6\_b\_implementation}} |

CP-6 (1) Control Enhancement (M) (H)

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

| CP-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_6\_1\_role}} | |
| {{cp\_6\_1\_status}} | |
| {{cp\_6\_1\_origination}} | |

| CP-6 (1) What is the solution and how is it implemented? |
| --- |
| {{cp\_6\_1\_implementation}} |

CP-6 (2) Control Enhancement (H)

The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

| CP-6 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_6\_2\_role}} | |
| {{cp\_6\_2\_status}} | |
| {{cp\_6\_2\_origination}} | |

| CP-6 (2) What is the solution and how is it implemented? |
| --- |
| {{cp\_6\_2\_implementation}} |

CP-6 (3) Control Enhancement (M) (H)

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

| CP-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_6\_3\_role}} | |
| {{cp\_6\_3\_status}} | |
| {{cp\_6\_3\_origination}} | |

| CP-6 (3) What is the solution and how is it implemented? |
| --- |
| {{cp\_6\_3\_implementation}} |

CP-7 Alternate Processing Site (M) (H)

The organization:

1. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined information system operations*] for essential missions/business functions within [*FedRAMP Assignment: see additional FedRAMP requirements and guidance*] when the primary processing capabilities are unavailable;

**CP-7a Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

1. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
2. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

| CP-7 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_7\_role}} | |
| Parameter CP-7(a)-1: {{cp\_7\_a\_1\_parameter}} | |
| Parameter CP-7(a)-2: {{cp\_7\_a\_2\_parameter}} | |
| {{cp\_7\_status}} | |
| {{cp\_7\_origination}} | |

| CP-7 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cp\_7\_a\_implementation}} |
| **Part b** | {{cp\_7\_b\_implementation}} |
| **Part c** | {{cp\_7\_c\_implementation}} |

CP-7 (1) Control Enhancement (M) (H)

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

**CP-7(1) Additional FedRAMP Requirements and Guidance**

**Guidance:** The service provider may determine what is considered a sufficient degree of separation between the primary and alternate processing sites, based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites will be less relevant.

| CP-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_7\_1\_role}} | |
| {{cp\_7\_1\_status}} | |
| {{cp\_7\_1\_origination}} | |

| CP-7 (1) What is the solution and how is it implemented? |
| --- |
| {{cp\_7\_1\_implementation}} |

CP-7 (2) Control Enhancement (M) (H)

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

| CP-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_7\_2\_role}} | |
| {{cp\_7\_2\_status}} | |
| {{cp\_7\_2\_origination}} | |

| CP-7 (2) What is the solution and how is it implemented? |
| --- |
| {{cp\_7\_2\_implementation}} |

CP-7 (3) Control Enhancement (M) (H)

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

| CP-7 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_7\_3\_role}} | |
| {{cp\_7\_3\_status}} | |
| {{cp\_7\_3\_origination}} | |

| CP-7 (3) What is the solution and how is it implemented? |
| --- |
| {{cp\_7\_3\_implementation}} |

CP-7 (4) Control Enhancement (H)

The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

| CP-7 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_7\_4\_role}} | |
| {{cp\_7\_4\_status}} | |
| {{cp\_7\_4\_origination}} | |

| CP-7 (4) What is the solution and how is it implemented? |
| --- |
| {{cp\_7\_4\_implementation}} |

CP-8 Telecommunications Services (M) (H)

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*Assignment: organization-defined information system operations*] for essential missions and business functions within [*FedRAMP Assignment: See CP-8 additional FedRAMP requirements and guidance*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

**CP-8 Additional FedRAMP Requirements and Guidance**:

**Requirement:** The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

| CP-8 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_8\_role}} | |
| Parameter CP-8-1: {{cp\_8\_1\_parameter}} | |
| Parameter CP-8-2: {{cp\_8\_2\_parameter}} | |
| {{cp\_8\_status}} | |
| {{cp\_8\_origination}} | |

| CP-8 What is the solution and how is it implemented? |
| --- |
| {{cp\_8\_implementation}} |

CP-8 (1) Control Enhancement (M) (H)

The organization:

1. Develops primary and alternate telecommunications service agreements that contain priority- of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
2. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

| CP-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_8\_1\_role}} | |
| {{cp\_8\_1\_status}} | |
| {{cp\_8\_1\_origination}} | |

| CP-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cp\_8\_1\_a\_implementation}} |
| **Part b** | {{cp\_8\_1\_b\_implementation}} |

CP-8 (2) Control Enhancement (M) (H)

The organization obtains 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: {{cp\_8\_2\_role}} | |
| {{cp\_8\_2\_status}} | |
| {{cp\_8\_2\_origination}} | |

| CP-8 (2) What is the solution and how is it implemented? |
| --- |
| {{cp\_8\_2\_implementation}} |

CP-8 (3) Control Enhancement (H)

The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

| CP-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_8\_3\_role}} | |
| {{cp\_8\_3\_status}} | |
| {{cp\_8\_3\_origination}} | |

| CP-8 (3) What is the solution and how is it implemented? |
| --- |
| {{cp\_8\_3\_implementation}} |

CP-8 (4) Control Enhancement (H)

The organization:

1. Requires primary and alternate telecommunications service providers to have contingency plans;
2. Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and
3. Obtains evidence of contingency testing/training by providers [*FedRAMP Assignment: annually*].

| CP-8 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_8\_4\_role}} | |
| Parameter CP-8(4)(c): {{cp\_8\_4\_c\_parameter}} | |
| {{cp\_8\_4\_status}} | |
| {{cp\_8\_4\_origination}} | |

| CP-8 (4) What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cp\_8\_4\_a\_implementation}} |
| **Part b** | {{cp\_8\_4\_b\_implementation}} |
| **Part c** | {{cp\_8\_4\_c\_implementation}} |

CP-9 Information System Backup (L) (M) (H)

The organization:

**CP-9 Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider shall determine what elements of the cloud environment require the Information System Backup control. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check.

1. Conducts backups of user-level information contained in the information system [*FedRAMP Assignment: daily incremental; weekly full*]

**CP-9 (a) Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider maintains at least three backup copies of user-level information (at least one of which is available online).

1. Conducts backups of system-level information contained in the information system [*FedRAMP Assignment: daily incremental; weekly full*];

**CP-9 (b) Additional FedRAMP Requirements and Guidance:**

**Requirement**: The service provider maintains at least three backup copies of system-level information (at least one of which is available online).

1. Conducts backups of information system documentation including security-related documentation [*FedRAMP Assignment: daily incremental; weekly full]*; and

**CP-9 (c) Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online).

1. Protects the confidentiality, integrity, and availability of backup information at storage locations.

| CP-9 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_9\_role}} | |
| Parameter CP-09(a): {{cp\_9\_a\_parameter}} | |
| Parameter CP-09(b): {{cp\_9\_b\_parameter}} | |
| Parameter CP-09(c): {{cp\_9\_c\_parameter}} | |
| {{cp\_9\_status}} | |
| {{cp\_9\_origination}} | |

| CP-9 What is the solution and how is it implemented? | |
| --- | --- |
| **Part a** | {{cp\_9\_a\_implementation}} |
| **Part b** | {{cp\_9\_b\_implementation}} |
| **Part c** | {{cp\_9\_c\_implementation}} |
| **Part d** | {{cp\_9\_d\_implementation}} |

CP-9 (1) Control Enhancement (H)

The organization tests backup information [*FedRAMP Assignment: at least monthly*] to verify media reliability and information integrity.

| CP-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_9\_1\_role}} | |
| Parameter CP-09(1): {{cp\_9\_1\_parameter}} | |
| {{cp\_9\_1\_status}} | |
| {{cp\_9\_1\_origination}} | |

| CP-9 (1) What is the solution and how is it implemented? |
| --- |
| {{cp\_9\_1\_implementation}} |

CP-9 (2) Control Enhancement (H)

The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

| CP-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_9\_2\_role}} | |
| {{cp\_9\_2\_status}} | |
| {{cp\_9\_2\_origination}} | |

| CP-9 (2) What is the solution and how is it implemented? |
| --- |
| {{cp\_9\_2\_implementation}} |

CP-9 (3) Control Enhancement (M) (H)

The organization stores backup copies of [*Assignment: organization-defined critical information system software and other security-related information*] in a separate facility or in a fire-rated container that is not collocated with the operational system.

| CP-9 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_9\_3\_role}} | |
| Parameter CP-09(3): {{cp\_9\_3\_parameter}} | |
| {{cp\_9\_3\_status}} | |
| {{cp\_9\_3\_origination}} | |

| CP-9 (3) What is the solution and how is it implemented? |
| --- |
| {{cp\_9\_3\_implementation}} |

CP-9 (5) Control Enhancement (H)

The organization transfers information system backup information to the alternate storage site [*FedRAMP Assignment: time period and transfer rate consistent with the recovery time and recovery point objectives defined in the service provider and organization SLA*].

| CP-9 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_9\_5\_role}} | |
| Parameter CP-9 (5): {{cp\_9\_5\_parameter}} | |
| {{cp\_9\_5\_status}} | |
| {{cp\_9\_5\_origination}} | |

| CP-9 (5) What is the solution and how is it implemented? |
| --- |
| {{cp\_9\_5\_implementation}} |

CP-10 Information System Recovery and Reconstitution (L) (M) (H)

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

| CP-10 | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_10\_role}} | |
| {{cp\_10\_status}} | |
| {{cp\_10\_origination}} | |

| CP-10 What is the solution and how is it implemented? |
| --- |
| {{cp\_10\_implementation}} |

CP-10 (2) Control Enhancement (M) (H)

The information system implements transaction recovery for systems that are transaction-based.

| CP-10 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_10\_2\_role}} | |
| {{cp\_10\_2\_status}} | |
| {{cp\_10\_2\_origination}} | |

| CP-10 (2) What is the solution and how is it implemented? |
| --- |
| {{cp\_10\_2\_implementation}} |

CP-10 (4) Control Enhancement (H)

The organization provides the capability to restore information system components within [*FedRAMP Assignment: time period consistent with the restoration time-periods defined in the service provider and organization SLA*] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

| CP-10 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{cp\_10\_4\_role}} | |
| Parameter CP-10 (4): {{cp\_10\_4\_parameter}} | |
| {{cp\_10\_4\_status}} | |
| {{cp\_10\_4\_origination}} | |

| CP-10 (4) What is the solution and how is it implemented? |
| --- |
| {{cp\_10\_4\_implementation}} |

## Identification and Authentication (IA)

IA-1 Identification and Authentication Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

(b) Reviews and updates the current:

* 1. Identification and authentication policy [*FedRAMP Assignment: at least annually*; and
  2. Identification and authentication procedures [*FedRAMP Assignment: at least annually*].

| IA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_1\_role}} | |
| Parameter IA-1(a): {{ia\_1\_a\_parameter}} | |
| Parameter IA-1(b)(1): {{ia\_1\_b\_1\_parameter}} | |
| Parameter IA-1(b)(2): {{ia\_1\_b\_2\_parameter}} | |
| {{ia\_1\_status}} | |
| {{ia\_1\_origination}} | |

| **IA-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ia\_1\_a\_implementation}} |
| **Part b** | {{ia\_1\_b\_implementation}} |

IA-2 User Identification and Authentication (L) (M) (H)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

| IA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_2\_role}} | |
| {{ia\_2\_status}} | |
| {{ia\_2\_origination}} | |

| **IA-2 What is the solution and how is it implemented?** |
| --- |
| {{ia\_2\_implementation}} |

IA-2 (1) Control Enhancement (L) (M) (H)

The information system implements multifactor authentication for network access to privileged accounts.

| IA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_2\_1\_role}} | |
| {{ia\_2\_1\_status}} | |
| {{ia\_2\_1\_origination}} | |

| **IA-2 (1) What is the solution and how is it implemented?** |
| --- |
| {{ia\_2\_1\_implementation}} |

IA-2 (2) Control Enhancement (M) (H)

The information system implements multifactor authentication for network access to non-privileged accounts.

| IA-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_2\_2\_role}} | |
| {{ia\_2\_2\_status}} | |
| {{ia\_2\_2\_origination}} | |

| **IA-2 (2) What is the solution and how is it implemented?** |
| --- |
| {{ia\_2\_2\_implementation}} |

IA-2 (3) Control Enhancement (M) (H)

The information system implements multifactor authentication for local access to privileged accounts.

| IA-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_2\_3\_role}} | |
| {{ia\_2\_3\_status}} | |
| {{ia\_2\_3\_origination}} | |

| **IA-2 (3) What is the solution and how is it implemented?** |
| --- |
| {{ia\_2\_3\_implementation}} |

IA-2 (4) Control Enhancement (H)

The information system implements multifactor authentication for local access to non-privileged accounts.

| IA-2 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_2\_4\_role}} | |
| {{ia\_2\_4\_status}} | |
| {{ia\_2\_4\_origination}} | |

| **IA-2 (4) What is the solution and how is it implemented?** |
| --- |
| {{ia\_2\_4\_implementation}} |

IA-2 (5) Control Enhancement (M) (H)

The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

| IA-2 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_2\_5\_role}} | |
| {{ia\_2\_5\_status}} | |
| {{ia\_2\_5\_origination}} | |

| **IA-2 (5) What is the solution and how is it implemented?** |
| --- |
| {{ia\_2\_5\_implementation}} |

IA-2 (8) Control Enhancement (M) (H)

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

| IA-2 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_2\_8\_role}} | |
| {{ia\_2\_8\_status}} | |
| {{ia\_2\_8\_origination}} | |

| **IA-2 (8) What is the solution and how is it implemented?** |
| --- |
| {{ia\_2\_8\_implementation}} |

IA-2 (9) Control Enhancement (H)

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

| IA-2 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_2\_9\_role}} | |
| {{ia\_2\_9\_status}} | |
| {{ia\_2\_9\_origination}} | |

| **IA-2 (9) What is the solution and how is it implemented?** |
| --- |
| {{ia\_2\_9\_implementation}} |

IA-2 (11) Control Enhancement (M) (H)

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*FedRAMP* *Assignment: FIPS 140-2, NIAP\* Certification, or NSA approval*].

\*National Information Assurance Partnership (NIAP)

**Additional FedRAMP Requirements and Guidance:**

**Guidance:** PIV = separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials. FIPS 140-2 means validated by the Cryptographic Module Validation Program (CMVP).

| IA-2 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_2\_11\_role}} | |
| Parameter IA-02(11): {{ia\_2\_11\_parameter}} | |
| {{ia\_2\_11\_status}} | |
| {{ia\_2\_11\_origination}} | |

| **IA-2 (11) What is the solution and how is it implemented?** |
| --- |
| {{ia\_2\_11\_implementation}} |

IA-2 (12) Control Enhancement (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

**IA-2 (12) Additional FedRAMP Requirements and Guidance**:

**Guidance**: Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12.

| IA-2 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_2\_12\_role}} | |
| {{ia\_2\_12\_status}} | |
| {{ia\_2\_12\_origination}} | |

| **IA-2 (12) What is the solution and how is it implemented?** |
| --- |
| {{ia\_2\_12\_implementation}} |

IA-3 Device Identification and Authentication (M) (H)

The information system uniquely identifies and authenticates [*Assignment: organization-defined specific and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection.

| IA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_3\_role}} | |
| Parameter IA-3(1): {{ia\_3\_1\_parameter}} | |
| Parameter IA-3-2: {{ia\_3\_2\_parameter}} | |
| {{ia\_3\_status}} | |
| {{ia\_3\_origination}} | |

| **IA-3 What is the solution and how is it implemented?** |
| --- |
| {{ia\_3\_implementation}} |

IA-4 Identifier Management (H)

The organization manages information system identifiers for users and devices by:

1. Receiving authorization from [*FedRAMP Assignment at a minimum, the ISSO (or similar role within the organization)*] to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for [*FedRAMP Assignment: at least two (2) years*]; and
5. Disabling the identifier after [*FedRAMP Assignment: thirty-five (35) days (see additional requirements and guidance)*]

**IA-4e Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider defines the time period of inactivity for device identifiers.

**Guidance:** For DoD clouds, see DoD cloud website for specific DoD requirements that go above and beyond FedRAMP <http://iase.disa.mil/cloud_security/Pages/index.aspx>.

| IA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_4\_role}} | |
| Parameter IA-04(a): {{ia\_4\_a\_parameter}} | |
| Parameter IA-04(d): {{ia\_4\_d\_parameter}} | |
| Parameter IA-04(e): {{ia\_4\_e\_parameter}} | |
| {{ia\_4\_status}} | |
| {{ia\_4\_origination}} | |

| **IA-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ia\_4\_a\_implementation}} |
| **Part b** | {{ia\_4\_b\_implementation}} |
| **Part c** | {{ia\_4\_c\_implementation}} |
| **Part d** | {{ia\_4\_d\_implementation}} |
| **Part e** | {{ia\_4\_e\_implementation}} |

IA-4 (4) Control Enhancement (M) (H)

The organization manages individual identifiers by uniquely identifying each individual as [*FedRAMP* *Assignment: contractors; foreign nationals*].

| IA-4 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_4\_4\_role}} | |
| Parameter IA-04(4): {{ia\_4\_4\_parameter}} | |
| {{ia\_4\_4\_status}} | |
| {{ia\_4\_4\_origination}} | |

| **IA-4 (4) What is the solution and how is it implemented?** |
| --- |
| {{ia\_4\_4\_implementation}} |

IA-5 Authenticator Management (H)

The organization manages information system authenticators by:

1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
2. Establishing initial authenticator content for authenticators defined by the organization;
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
5. Changing default content of authenticators prior to information system installation;
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
7. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*].
8. Protecting authenticator content from unauthorized disclosure and modification;
9. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
10. Changing authenticators for group/role accounts when membership to those accounts’ changes.

**IA-5 Additional FedRAMP Requirements and Guidance:**

**Requirement:** Authenticators must be compliant with NIST SP 800-63-3 Digital Identity Guidelines IAL, AAL, FAL level 3. Link <https://pages.nist.gov/800-63-3>

| IA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_5\_role}} | |
| Parameter IA-05(g): {{ia\_5\_g\_parameter}} | |
| {{ia\_5\_status}} | |
| {{ia\_5\_origination}} | |

| **IA-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ia\_5\_a\_implementation}} |
| **Part b** | {{ia\_5\_b\_implementation}} |
| **Part c** | {{ia\_5\_c\_implementation}} |
| **Part d** | {{ia\_5\_d\_implementation}} |
| **Part e** | {{ia\_5\_e\_implementation}} |
| **Part f** | {{ia\_5\_f\_implementation}} |
| **Part g** | {{ia\_5\_g\_implementation}} |
| **Part h** | {{ia\_5\_h\_implementation}} |
| **Part i** | {{ia\_5\_i\_implementation}} |
| **Part j** | {{ia\_5\_j\_implementation}} |

IA-5 (1) Control Enhancement (H)

The information system, for password-based authentication:

1. Enforces minimum password complexity of [*Assignment:* *organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];
2. Enforces at least the following number of changed characters when new passwords are created: [*FedRAMP* *Assignment: at least fifty percent (50%)*];
3. Stores and transmits only cryptographically protected passwords;
4. Enforces password minimum and maximum lifetime restrictions of [*Assignment: organization- defined numbers for lifetime minimum, lifetime maximum*];
5. Prohibits password reuse for [*FedRAMP Assignment: twenty-four (24)*] generations; and
6. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

**IA-5 (1) a and d Additional FedRAMP Requirements and Guidance:**

**Guidance:** If password policies are compliant with NIST SP 800-63B Memorized Secret (Section 5.1.1) Guidance, the control may be considered compliant.

| IA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_5\_1\_role}} | |
| Parameter IA-05(1)(a): {{ia\_5\_1\_a\_parameter}} | |
| Parameter IA-05(1)(b): {{ia\_5\_1\_b\_parameter}} | |
| Parameter IA-05(1)(d): {{ia\_5\_1\_d\_parameter}} | |
| Parameter IA-05(1)(e): {{ia\_5\_1\_e\_parameter}} | |
| {{ia\_5\_1\_status}} | |
| {{ia\_5\_1\_origination}} | |

| **IA-5 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ia\_5\_1\_a\_implementation}} |
| **Part b** | {{ia\_5\_1\_b\_implementation}} |
| **Part c** | {{ia\_5\_1\_c\_implementation}} |
| **Part d** | {{ia\_5\_1\_d\_implementation}} |
| **Part e** | {{ia\_5\_1\_e\_implementation}} |
| **Part f** | {{ia\_5\_1\_f\_implementation}} |

IA-5 (2) Control Enhancement (M) (H)

The information system, for PKI-based authentication:

1. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
2. Enforces authorized access to the corresponding private key;
3. Maps the authenticated identity to the account of the individual or group; and
4. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

| IA-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_5\_2\_role}} | |
| {{ia\_5\_2\_status}} | |
| {{ia\_5\_2\_origination}} | |

| **IA-5 (2) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ia\_5\_2\_a\_implementation}} |
| **Part b** | {{ia\_5\_2\_b\_implementation}} |
| **Part c** | {{ia\_5\_2\_c\_implementation}} |
| **Part d** | {{ia\_5\_2\_d\_implementation}} |

IA-5 (3) Control Enhancement (M) (H)

The organization requires that the registration process to receive [*FedRAMP* *Assignment: All hardware/biometric (multifactor authenticators*] be conducted [*FedRAMP* *Selection: in person*] before [*Assignment: organization-defined registration authority*] with authorization by [*Assignment: organization-defined personnel or roles*].

| IA-5 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_5\_3\_role}} | |
| Parameter IA-5(3)(1): {{ia\_5\_3\_1\_parameter}} | |
| Parameter IA-5(3)(2): {{ia\_5\_3\_2\_parameter}} | |
| Parameter IA-5(3)(3): {{ia\_5\_3\_3\_parameter}} | |
| Parameter IA-5(3)(4): {{ia\_5\_3\_4\_parameter}} | |
| {{ia\_5\_3\_status}} | |
| {{ia\_5\_3\_origination}} | |

| **IA-5 (3) What is the solution and how is it implemented?** |
| --- |
| {{ia\_5\_3\_implementation}} |

IA-5 (4) Control Enhancement (H)

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*FedRAMP Assignment: complexity as identified in IA-5 (1) Control Enhancement (H) Part A*].

**IA-5(4) Additional FedRAMP Requirements and Guidance:**

**Guidance:** If automated mechanisms which enforce password authenticator strength at creation are not used, automated mechanisms must be used to audit strength of created password authenticators.

| IA-5 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_5\_4\_role}} | |
| Parameter IA-05(4): {{ia\_5\_4\_parameter}} | |
| {{ia\_5\_4\_status}} | |
| {{ia\_5\_4\_origination}} | |

| **IA-5 (4) What is the solution and how is it implemented?** |
| --- |
| {{ia\_5\_4\_implementation}} |

IA-5 (6) Control Enhancement (M) (H)

The organization protects 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: {{ia\_5\_6\_role}} | |
| {{ia\_5\_6\_status}} | |
| {{ia\_5\_6\_origination}} | |

| **IA-5 (6) What is the solution and how is it implemented?** |
| --- |
| {{ia\_5\_6\_implementation}} |

IA-5 (7) Control Enhancement (M) (H)

The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

| IA-5 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_5\_7\_role}} | |
| {{ia\_5\_7\_status}} | |
| {{ia\_5\_7\_origination}} | |

| **IA-5 (7) What is the solution and how is it implemented?** |
| --- |
| {{ia\_5\_7\_implementation}} |

IA-5 (8) Control Enhancement (H)

The organization implements [*FedRAMP Assignment: different authenticators on different systems*] to manage the risk of compromise due to individuals having accounts on multiple information systems.

| IA-5 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_5\_8\_role}} | |
| Parameter IA-5 (8): {{ia\_5\_8\_parameter}} | |
| {{ia\_5\_8\_status}} | |
| {{ia\_5\_8\_origination}} | |

| **IA-5 (8) What is the solution and how is it implemented?** |
| --- |
| {{ia\_5\_8\_implementation}} |

IA-5 (11) Control Enhancement (L) (M) (H)

The information system, for hardware token-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined token quality* requirements*].*

| IA-5 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_5\_11\_role}} | |
| Parameter IA-05(11): {{ia\_5\_11\_parameter}} | |
| {{ia\_5\_11\_status}} | |
| {{ia\_5\_11\_origination}} | |

| **IA-5 (11) What is the solution and how is it implemented?** |
| --- |
| {{ia\_5\_11\_implementation}} |

IA-5 (13) Control Enhancement (H)

The information system prohibits the use of cached authenticators after [*Assignment: organization-defined time period*].

| IA-5 (13) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_5\_13\_role}} | |
| Parameter IA-5 (13): {{ia\_5\_13\_parameter}} | |
| {{ia\_5\_13\_status}} | |
| {{ia\_5\_13\_origination}} | |

| **IA-5 (13) What is the solution and how is it implemented?** |
| --- |
| {{ia\_5\_13\_implementation}} |

IA-6 Authenticator Feedback (L) (M) (H)

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

| IA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_6\_role}} | |
| {{ia\_6\_status}} | |
| {{ia\_6\_origination}} | |

| **IA-6 What is the solution and how is it implemented?** |
| --- |
| {{ia\_6\_implementation}} |

IA-7 Cryptographic Module Authentication (L) (M) (H)

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

| IA-7 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_7\_role}} | |
| {{ia\_7\_status}} | |
| {{ia\_7\_origination}} | |

| **IA-7 What is the solution and how is it implemented?** |
| --- |
| {{ia\_7\_implementation}} |

IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H)

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

| IA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_8\_role}} | |
| {{ia\_8\_status}} | |
| {{ia\_8\_origination}} | |

| **IA-8 What is the solution and how is it implemented?** |
| --- |
| {{ia\_8\_implementation}} |

IA-8 (1) Control Enhancement (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

| IA-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_8\_1\_role}} | |
| {{ia\_8\_1\_status}} | |
| {{ia\_8\_1\_origination}} | |

| **IA-8 (1) What is the solution and how is it implemented?** |
| --- |
| {{ia\_8\_1\_implementation}} |

IA-8 (2) Control Enhancement (L) (M) (H)

The information system accepts only FICAM-approved third-party credentials.

| IA-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_8\_2\_role}} | |
| {{ia\_8\_2\_status}} | |
| {{ia\_8\_2\_origination}} | |

| **IA-8 (2) What is the solution and how is it implemented?** |
| --- |
| {{ia\_8\_2\_implementation}} |

IA-8 (3) Control Enhancement (L) (M) (H)

The organization employs only FICAM-approved information system components in [*Assignment: organization-defined information systems*] to accept third-party credentials.

| IA-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_8\_3\_role}} | |
| Parameter IA-08(3): {{ia\_8\_3\_parameter}} | |
| {{ia\_8\_3\_status}} | |
| {{ia\_8\_3\_origination}} | |

| **IA-8 (3) What is the solution and how is it implemented?** |
| --- |
| {{ia\_8\_3\_implementation}} |

IA-8 (4) Control Enhancement (L) (M) (H)

The information system conforms to FICAM-issued profiles.

| IA-8 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ia\_8\_4\_role}} | |
| {{ia\_8\_4\_status}} | |
| {{ia\_8\_4\_origination}} | |

| **IA-8 (4) What is the solution and how is it implemented?** |
| --- |
| {{ia\_8\_4\_implementation}} |

## Incident Response (IR)

IR-1 Incident Response Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
2. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
4. Reviews and updates the current:
5. Incident response policy [*FedRAMP Assignment: at least annually*]; and
6. Incident response procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| IR-1 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_1\_role}} | |
| Parameter IR-01(a): {{ir\_1\_a\_parameter}} | |
| Parameter IR-01(b)(1): {{ir\_1\_b\_1\_parameter}} | |
| Parameter IR-01(b)(2): {{ir\_1\_b\_2\_parameter}} | |
| {{ir\_1\_status}} | |
| {{ir\_1\_origination}} | |

| **IR-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ir\_1\_a\_implementation}} |
| **Part b** | {{ir\_1\_b\_implementation}} |

IR-2 Incident Response Training (H)

The organization provides incident response training to information system users consistent with assigned roles and responsibilities in accordance with NIST SP 800-53 Rev 4:

1. Within [*FedRAMP Assignment: ten (10) days*] of assuming an incident response role or responsibility;
2. When required by information system changes; and
3. [*FedRAMP Assignment: at least annually*] thereafter.

| IR-2 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_2\_role}} | |
| Parameter IR-02(a): {{ir\_2\_a\_parameter}} | |
| Parameter IR-02(c): {{ir\_2\_c\_parameter}} | |
| {{ir\_2\_status}} | |
| {{ir\_2\_origination}} | |

| **IR-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ir\_2\_a\_implementation}} |
| **Part b** | {{ir\_2\_b\_implementation}} |
| **Part c** | {{ir\_2\_c\_implementation}} |

IR-2 (1) Control Enhancement (H)

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

| IR-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_2\_1\_role}} | |
| {{ir\_2\_1\_status}} | |
| {{ir\_2\_1\_origination}} | |

| **IR-2 (1) What is the solution and how is it implemented?** |
| --- |
| {{ir\_2\_1\_implementation}} |

IR-2 (2) Control Enhancement (H)

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

| IR-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_2\_2\_role}} | |
| {{ir\_2\_2\_status}} | |
| {{ir\_2\_2\_origination}} | |

| **IR-2 (2) What is the solution and how is it implemented?** |
| --- |
| {{ir\_2\_2\_implementation}} |

IR-3 Incident Response Testing (H)

The organization tests the incident response capability for the information system [*FedRAMP Assignment: at least every six (6) months*] to determine the incident response effectiveness and documents the results.

**IR-3 Additional FedRAMP Requirements and Guidance:**

**Requirements:** The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). For JAB authorization, the service provider provides test plans to the JAB/AO annually. Test plans are approved and accepted by the JAB/AO prior to the test commencing.

| IR-3 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_3\_role}} | |
| Parameter IR-3-1: {{ir\_3\_1\_parameter}} | |
| Parameter IR-3-2: {{ir\_3\_2\_parameter}} | |
| {{ir\_3\_status}} | |
| {{ir\_3\_origination}} | |

| **IR-3 What is the solution and how is it implemented?** |
| --- |
| {{ir\_3\_implementation}} |

IR-3 (2) Control Enhancement (M) (H)

The organization coordinates incident response testing with organizational elements responsible for related plans.

| IR-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_3\_2\_role}} | |
| {{ir\_3\_2\_status}} | |
| {{ir\_3\_2\_origination}} | |

| **IR-3 (2) What is the solution and how is it implemented?** |
| --- |
| {{ir\_3\_2\_implementation}} |

IR-4 Incident Handling (L) (M) (H)

The organization:

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
2. Coordinates incident handling activities with contingency planning activities; and
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

**IR-4 Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

| IR-4 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_4\_role}} | |
| {{ir\_4\_status}} | |
| {{ir\_4\_origination}} | |

| **IR-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ir\_4\_a\_implementation}} |
| **Part b** | {{ir\_4\_b\_implementation}} |
| **Part c** | {{ir\_4\_c\_implementation}} |

IR-4 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to support the incident handling process.

| IR-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_4\_1\_role}} | |
| {{ir\_4\_1\_status}} | |
| {{ir\_4\_1\_origination}} | |

| **IR-4 (1) What is the solution and how is it implemented?** |
| --- |
| {{ir\_4\_1\_implementation}} |

IR-4 (2) Control Enhancement (H)

The organization includes dynamic reconfiguration of [*FedRAMP Assignment: all network, data storage, and computing devices*] as part of the incident response capability.

| IR-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_4\_2\_role}} | |
| Parameter IR-4 (2): {{ir\_4\_2\_parameter}} | |
| {{ir\_4\_2\_status}} | |
| {{ir\_4\_2\_origination}} | |

| **IR-4 (2) What is the solution and how is it implemented?** |
| --- |
| {{ir\_4\_2\_implementation}} |

IR-4 (3) Control Enhancement (H)

The organization identifies [*Assignment: organization-defined classes of incidents*] and [*Assignment: organization-defined actions to take in response to classes of incident*] to ensure continuation of organizational missions and business functions.

| IR-4 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_4\_3\_role}} | |
| Parameter IR-4 (3)-1: {{ir\_4\_3\_1\_parameter}} | |
| Parameter IR-4 (3)-2: {{ir\_4\_3\_2\_parameter}} | |
| {{ir\_4\_3\_status}} | |
| {{ir\_4\_3\_origination}} | |

| **IR-4 (3) What is the solution and how is it implemented?** | |
| --- | --- |
| **IR-4 (3)** | {{ir\_4\_3\_implementation}} |

IR-4 (4) Control Enhancement (H)

The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

| IR-4 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_4\_4\_role}} | |
| {{ir\_4\_4\_status}} | |
| {{ir\_4\_4\_origination}} | |

| **IR-4 (4) What is the solution and how is it implemented?** |
| --- |
| {{ir\_4\_4\_implementation}} |

IR-4 (6) Control Enhancement (H)

The organization implements incident handling capability for insider threats.

| IR-4 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_4\_6\_role}} | |
| {{ir\_4\_6\_status}} | |
| {{ir\_4\_6\_origination}} | |

| **IR-4 (6) What is the solution and how is it implemented?** |
| --- |
| {{ir\_4\_6\_implementation}} |

IR-4 (8) Control Enhancement (H)

The organization coordinates with [*FedRAMP Assignment: external organizations including consumer incident responders and network defenders and the appropriate consumer incident response team (CIRT)/* *Computer Emergency Response Team (CERT) (such as US-CERT, DoD CERT, IC CERT)*] to correlate and share [*Assignment: organization-defined incident information*] to achieve a cross- organization perspective on incident awareness and more effective incident responses.

| IR-4 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_4\_8\_role}} | |
| Parameter IR-4 (8)-1: {{ir\_4\_8\_1\_parameter}} | |
| Parameter IR-4 (8)-2: {{ir\_4\_8\_2\_parameter}} | |
| {{ir\_4\_8\_status}} | |
| {{ir\_4\_8\_origination}} | |

| **IR-4 (8) What is the solution and how is it implemented?** |
| --- |
| {{ir\_4\_8\_implementation}} |

IR-5 Incident Monitoring (L) (M) (H)

The organization tracks and documents information system security incidents.

| IR-5 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_5\_role}} | |
| {{ir\_5\_status}} | |
| {{ir\_5\_origination}} | |

| **IR-5 What is the solution and how is it implemented?** |
| --- |
| {{ir\_5\_implementation}} |

IR-5 (1) Control Enhancement (H)

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

| IR-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_5\_1\_role}} | |
| {{ir\_5\_1\_status}} | |
| {{ir\_5\_1\_origination}} | |

| **IR-5 (1) What is the solution and how is it implemented?** |
| --- |
| {{ir\_5\_1\_implementation}} |

IR-6 Incident Reporting (L) (M) (H)

The organization:

1. Requires personnel to report suspected security incidents to the organizational incident response capability within [*FedRAMP Assignment: US-CERT incident reporting timelines as specified in NIST SP800-61 (as amended)*]; and
2. Reports security incident information to [*Assignment: organization-defined authorities*].

**IR-6 Additional FedRAMP Requirements and Guidance**

**Requirement:** Report security incident information according to FedRAMP Incident Communications Procedure.

| IR-6 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_6\_role}} | |
| Parameter IR-06(a): {{ir\_6\_a\_parameter}} | |
| Parameter IR-06(b): {{ir\_6\_b\_parameter}} | |
| {{ir\_6\_status}} | |
| {{ir\_6\_origination}} | |

| **IR-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ir\_6\_a\_implementation}} |
| **Part b** | {{ir\_6\_b\_implementation}} |

IR-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to assist in the reporting of security incidents.

| IR-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_6\_1\_role}} | |
| {{ir\_6\_1\_status}} | |
| {{ir\_6\_1\_origination}} | |

| **IR-6 (1) What is the solution and how is it implemented?** |
| --- |
| {{ir\_6\_1\_implementation}} |

IR-7 Incident Response Assistance (L) (M) (H)

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

| IR-7 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_7\_role}} | |
| {{ir\_7\_status}} | |
| {{ir\_7\_origination}} | |

| **IR-7 What is the solution and how is it implemented?** |
| --- |
| {{ir\_7\_implementation}} |

IR-7 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to increase the availability of incident response related information and support.

| IR-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_7\_1\_role}} | |
| {{ir\_7\_1\_status}} | |
| {{ir\_7\_1\_origination}} | |

| **IR-7 (1) What is the solution and how is it implemented?** |
| --- |
| {{ir\_7\_1\_implementation}} |

IR-7 (2) Control Enhancement (M) (H)

The organization:

1. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and
2. Identifies organizational incident response team members to the external providers.

| IR-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_7\_2\_role}} | |
| {{ir\_7\_2\_status}} | |
| {{ir\_7\_2\_origination}} | |

| **IR-7 (2) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ir\_7\_2\_a\_implementation}} |
| **Part b** | {{ir\_7\_2\_b\_implementation}} |

IR-8 Incident Response Plan (L) (M) (H)

The organization:

1. Develops an incident response plan that:
2. Provides the organization with a roadmap for implementing its incident response capability;
3. Describes the structure and organization of the incident response capability;
4. Provides a high-level approach for how the incident response capability fits into the overall organization;
5. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
6. Defines reportable incidents;
7. Provides metrics for measuring the incident response capability within the organization;
8. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
9. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];
10. Distributes copies of the incident response plan to [*FedRAMP Assignment: see additional FedRAMP Requirements and Guidance*].

**IR-8(b) Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

1. Reviews the incident response plan [*FedRAMP Assignment: at least annually*];
2. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
3. Communicates incident response plan changes to [*FedRAMP Assignment: see additional FedRAMP Requirements and Guidance*].

**IR-8(e) Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

1. Protects the incident response plan from unauthorized disclosure and modification.

| IR-8 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_8\_role}} | |
| Parameter IR-08(a)(8): {{ir\_8\_a\_8\_parameter}} | |
| Parameter IR-08(b): {{ir\_8\_b\_parameter}} | |
| Parameter IR-08(c): {{ir\_8\_c\_parameter}} | |
| Parameter IR-08(e): {{ir\_8\_e\_parameter}} | |
| {{ir\_8\_status}} | |
| {{ir\_8\_origination}} | |

| **IR-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ir\_8\_a\_implementation}} |
| **Part b** | {{ir\_8\_b\_implementation}} |
| **Part c** | {{ir\_8\_c\_implementation}} |
| **Part d** | {{ir\_8\_d\_implementation}} |
| **Part e** | {{ir\_8\_e\_implementation}} |
| **Part f** | {{ir\_8\_f\_implementation}} |

IR-9 Information Spillage Response (M) (H)

The organization responds to information spills by:

1. Identifying the specific information involved in the information system contamination;
2. Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill;
3. Isolating the contaminated information system or system component;
4. Eradicating the information from the contaminated information system or component;
5. Identifying other information systems or system components that may have been subsequently contaminated; and
6. Performing other [*Assignment: organization-defined actions*].

| IR-9 | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_9\_role}} | |
| Parameter IR-09(b): {{ir\_9\_b\_parameter}} | |
| Parameter IR-09(f): {{ir\_9\_f\_parameter}} | |
| {{ir\_9\_status}} | |
| {{ir\_9\_origination}} | |

| **IR-9 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ir\_9\_a\_implementation}} |
| **Part b** | {{ir\_9\_b\_implementation}} |
| **Part c** | {{ir\_9\_c\_implementation}} |
| **Part d** | {{ir\_9\_d\_implementation}} |
| **Part e** | {{ir\_9\_e\_implementation}} |
| **Part f** | {{ir\_9\_f\_implementation}} |

IR-9 (1) Control Enhancement (M) (H)

The organization assigns [*Assignment: organization-defined personnel or roles*] with responsibility for responding to information spills.

| IR-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_9\_1\_role}} | |
| Parameter IR-09(1): {{ir\_9\_1\_parameter}} | |
| {{ir\_9\_1\_status}} | |
| {{ir\_9\_1\_origination}} | |

| **IR-9 (1) What is the solution and how is it implemented?** |
| --- |
| {{ir\_9\_1\_implementation}} |

IR-9 (2) Control Enhancement (M)

The organization provides information spillage response training [*FedRAMP Assignment: at least annually*].

| IR-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_9\_2\_role}} | |
| Parameter IR-09(2): {{ir\_9\_2\_parameter}} | |
| {{ir\_9\_2\_status}} | |
| {{ir\_9\_2\_origination}} | |

| **IR-9 (2) What is the solution and how is it implemented?** |
| --- |
| {{ir\_9\_2\_implementation}} |

IR-9 (3) Control Enhancement (M) (H)

The organization implements [*Assignment: organization-defined procedures*] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

| IR-9 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_9\_3\_role}} | |
| Parameter IR-09(3): {{ir\_9\_3\_parameter}} | |
| {{ir\_9\_3\_status}} | |
| {{ir\_9\_3\_origination}} | |

| **IR-9 (3) What is the solution and how is it implemented?** |
| --- |
| {{ir\_9\_3\_implementation}} |

IR-9 (4) Control Enhancement (M) (H)

The organization employs [*Assignment: organization-defined security safeguards*] for personnel exposed to information not within assigned access authorizations.

| IR-9 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: {{ir\_9\_4\_role}} | |
| Parameter IR-09(4): {{ir\_9\_4\_parameter}} | |
| {{ir\_9\_4\_status}} | |
| {{ir\_9\_4\_origination}} | |

| **IR-9 (4) What is the solution and how is it implemented?** |
| --- |
| {{ir\_9\_4\_implementation}} |

## Maintenance (MA)

MA-1 System Maintenance Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]*:
2. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
4. Reviews and updates the current:
   1. System maintenance policy [*FedRAMP Assignment: at least annually*]; and
   2. System maintenance procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| **MA-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ma\_1\_role}} | |
| Parameter MA-01(a): {{ma\_1\_a\_parameter}} | |
| Parameter MA-01(b)(1): {{ma\_1\_b\_1\_parameter}} | |
| Parameter MA-01(b)(2): {{ma\_1\_b\_2\_parameter}} | |
| {{ma\_1\_status}} | |
| {{ma\_1\_origination}} | |

| **MA-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ma\_1\_a\_implementation}} |
| **Part b** | {{ma\_1\_b\_implementation}} |

MA-2 Controlled Maintenance (L) (M) (H)

The organization:

1. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
2. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
3. Requires that [*Assignment: organization-defined personnel or roles*] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
4. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
5. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
6. Includes *[Assignment: organization-defined maintenance-related information*] in organizational maintenance records.

| **MA-2** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ma\_2\_role}} | |
| Parameter MA-2(c): {{ma\_2\_c\_parameter}} | |
| Parameter MA-2(f): {{ma\_2\_f\_parameter}} | |
| {{ma\_2\_status}} | |
| {{ma\_2\_origination}} | |

| **MA-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ma\_2\_a\_implementation}} |
| **Part b** | {{ma\_2\_b\_implementation}} |
| **Part c** | {{ma\_2\_c\_implementation}} |
| **Part d** | {{ma\_2\_d\_implementation}} |
| **Part e** | {{ma\_2\_e\_implementation}} |
| **Part f** | {{ma\_2\_f\_implementation}} |

MA-2 (2) Control Enhancement (H)

The organization:

1. Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and
2. Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

| **MA-2 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ma\_2\_2\_role}} | |
| {{ma\_2\_2\_status}} | |
| {{ma\_2\_2\_origination}} | |

| **MA-2 (2) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ma\_2\_2\_a\_implementation}} |
| **Part b** | {{ma\_2\_2\_b\_implementation}} |

MA-3 Maintenance Tools (M) (H)

The organization approves, controls, and monitors information system maintenance tools.

| **MA-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ma\_3\_role}} | |
| {{ma\_3\_status}} | |
| {{ma\_3\_origination}} | |

| **MA-3 What is the solution and how is it implemented?** |
| --- |
| {{ma\_3\_implementation}} |

MA-3 (1) Control Enhancement (M) (H)

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

| **MA-3 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ma\_3\_1\_role}} | |
| {{ma\_3\_1\_status}} | |
| {{ma\_3\_1\_origination}} | |

| **MA-3 (1) What is the solution and how is it implemented?** |
| --- |
| {{ma\_3\_1\_implementation}} |

MA-3 (2) Control Enhancement (M) (H)

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

| **MA-3 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ma\_3\_2\_role}} | |
| {{ma\_3\_2\_status}} | |
| {{ma\_3\_2\_origination}} | |

| **MA-3 (2) What is the solution and how is it implemented?** |
| --- |
| {{ma\_3\_2\_implementation}} |

MA-3 (3) Control Enhancement (M) (H)

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

1. Verifying that there is no organizational information contained on the equipment;
2. Sanitizing or destroying the equipment;
3. Retaining the equipment within the facility; or
4. Obtaining an exemption from [*FedRAMP Assignment: the information owner explicitly authorizes removal of the equipment from the facility*].

| **MA-3 (3)** | | **Control Summary Information** |
| --- | --- | --- |
| Responsible Role: {{ma\_3\_3\_role}} | | |
| Parameter MA-03(3)(d): {{ma\_3\_3\_d\_parameter}} | | |
| {{ma\_3\_3\_status}} | | |
| {{ma\_3\_3\_origination}} | | |
| **MA-3 (3) What is the solution and how is it implemented?** | | |
| **Part a** | {{ma\_3\_3\_a\_implementation}} | |
| **Part b** | {{ma\_3\_3\_b\_implementation}} | |
| **Part c** | {{ma\_3\_3\_c\_implementation}} | |
| **Part d** | {{ma\_3\_3\_d\_implementation}} | |

MA-4 Remote Maintenance (L) (M) (H)

The organization:

1. Approves and monitors nonlocal maintenance and diagnostic activities;
2. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
3. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
4. Maintains records for nonlocal maintenance and diagnostic activities; and
5. Terminates session and network connections when nonlocal maintenance is completed.

| **MA-4** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ma\_4\_role}} | |
| {{ma\_4\_status}} | |
| {{ma\_4\_origination}} | |

| **MA-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ma\_4\_a\_implementation}} |
| **Part b** | {{ma\_4\_b\_implementation}} |
| **Part c** | {{ma\_4\_c\_implementation}} |
| **Part d** | {{ma\_4\_d\_implementation}} |
| **Part e** | {{ma\_4\_e\_implementation}} |

MA-4 (2) Control Enhancement (M) (H)

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

| **MA-4 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ma\_4\_2\_role}} | |
| {{ma\_4\_2\_status}} | |
| {{ma\_4\_2\_origination}} | |

| **MA-4 (2) What is the solution and how is it implemented?** |
| --- |
| {{ma\_4\_2\_implementation}} |

MA-4 (3) Control Enhancement (H)

The organization:

1. Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or
2. Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.

| **MA-4 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ma\_4\_3\_role}} | |
| {{ma\_4\_3\_status}} | |
| {{ma\_4\_3\_origination}} | |

| **MA-4 (3) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ma\_4\_3\_a\_implementation}} |
| **Part b** | {{ma\_4\_3\_b\_implementation}} |

MA-4 (6) Control Enhancement (H)

The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.

| **MA-4 (6)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ma\_4\_6\_role}} | |
| {{ma\_4\_6\_status}} | |
| {{ma\_4\_6\_origination}} | |

| **MA-4 (6) What is the solution and how is it implemented?** |
| --- |
| {{ma\_4\_6\_implementation}} |

MA-5 Maintenance Personnel (L) (M) (H)

The organization:

1. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
2. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
3. Designates 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: {{ma\_5\_role}} | |
| {{ma\_5\_status}} | |
| {{ma\_5\_origination}} | |

| **MA-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ma\_5\_a\_implementation}} |
| **Part b** | {{ma\_5\_b\_implementation}} |
| **Part c** | {{ma\_5\_c\_implementation}} |

MA-5 (1) Control Enhancement (H)

The organization:

1. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
   1. 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 information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
   2. 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 information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
2. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.  
     
    MA-5 (1) Additional FedRAMP Requirements and Guidance:   
    Requirement: Only MA-5 (1) (a) (1) is required by FedRAMP

| **MA-5 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ma\_5\_1\_role}} | |
| {{ma\_5\_1\_status}} | |
| {{ma\_5\_1\_origination}} | |

| **MA-5 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ma\_5\_1\_a\_implementation}} |
| **Part b** | {{ma\_5\_1\_b\_implementation}} |

MA-6 Timely Maintenance (M) (H)

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

| **MA-6** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ma\_6\_role}} | |
| Parameter MA-6(1): {{ma\_6\_1\_parameter}} | |
| Parameter MA-6(2): {{ma\_6\_2\_parameter}} | |
| {{ma\_6\_status}} | |
| {{ma\_6\_origination}} | |

| **MA-6 What is the solution and how is it implemented?** |
| --- |
| {{ma\_6\_implementation}} |

## Media Protection (MP)

MP-1 Media Protection Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
2. Reviews and updates the current:
   1. Media protection policy [*FedRAMP Assignment: at least annually*]; and
   2. Media protection procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| **MP-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{mp\_1\_role}} | |
| Parameter MP-01(a): {{mp\_1\_a\_parameter}} | |
| Parameter MP-01(b)(1): {{mp\_1\_b\_1\_parameter}} | |
| Parameter MP-01(b)(2): {{mp\_1\_b\_2\_parameter}} | |
| {{mp\_1\_status}} | |
| {{mp\_1\_origination}} | |

| **MP-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{mp\_1\_a\_implementation}} |
| **Part b** | {{mp\_1\_b\_implementation}} |

MP-2 Media Access (H)

The organization restricts access to [*FedRAMP Assignment: any digital and non-digital media deemed sensitive*] to [*Assignment: organization-defined personnel or roles*].

| **MP-2** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{mp\_2\_role}} | |
| Parameter MP-2-1: {{mp\_2\_1\_parameter}} | |
| Parameter MP-2-2: {{mp\_2\_2\_parameter}} | |
| {{mp\_2\_status}} | |
| {{mp\_2\_origination}} | |

| **MP-2 What is the solution and how is it implemented?** |
| --- |
| {{mp\_2\_implementation}} |

MP-3 Media Labeling (M) (H)

The organization:

1. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
2. Exempts [*FedRAMP Assignment: no removable media types]* from marking as long as the media remain within [*Assignment: organization-defined controlled areas*].

**MP-3(b) Additional FedRAMP Requirements and Guidance:**

**Guidance:** Second parameter in MP-3(b)-2 is not applicable.

| **MP-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{mp\_3\_role}} | |
| Parameter MP-3(b)-1: {{mp\_3\_b\_1\_parameter}} | |
| Parameter MP-3(b)-2: {{mp\_3\_b\_2\_parameter}} | |
| {{mp\_3\_status}} | |
| {{mp\_3\_origination}} | |

| **MP-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{mp\_3\_a\_implementation}} |
| **Part b** | {{mp\_3\_b\_implementation}} |

MP-4 Media Storage (M) (H)

The organization:

1. Physically controls and securely stores [*FedRAMP Assignment: [all types of digital and non-digital media with sensitive information*] within [*FedRAMP Assignment: see additional FedRAMP requirements and guidance*]; and

**MP-4a Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider defines controlled areas within facilities where the information and information system reside.

1. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

| **MP-4** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{mp\_4\_role}} | |
| Parameter MP-4(a)-1: {{mp\_4\_a\_1\_parameter}} | |
| Parameter MP-4(a)-2: {{mp\_4\_a\_2\_parameter}} | |
| {{mp\_4\_status}} | |
| {{mp\_4\_origination}} | |

| **MP-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{mp\_4\_a\_implementation}} |
| **Part b** | {{mp\_4\_b\_implementation}} |

MP-5 Media Transport (M) (H)

The organization:

1. Protects and controls [*FedRAMP Assignment: all media with sensitive information*] during transport outside of controlled areas using [*FedRAMP Assignment:* *for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secured in locked container*];

**MP-5a Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB/AO.

1. Maintains accountability for information system media during transport outside of controlled areas;
2. Documents activities associated with the transport of information system media; and
3. Restricts the activities associated with transport of information system media to authorized personnel.

| **MP-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{mp\_5\_role}} | |
| Parameter MP-5(a)-1: {{mp\_5\_a\_1\_parameter}} | |
| Parameter MP-5(a)-2: {{mp\_5\_a\_2\_parameter}} | |
| {{mp\_5\_status}} | |
| {{mp\_5\_origination}} | |

| **MP-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{mp\_5\_a\_implementation}} |
| **Part b** | {{mp\_5\_b\_implementation}} |
| **Part c** | {{mp\_5\_c\_implementation}} |
| **Part d** | {{mp\_5\_d\_implementation}} |

MP-5 (4) Control Enhancement (M) (H)

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

| **MP-5 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{mp\_5\_4\_role}} | |
| {{mp\_5\_4\_status}} | |
| {{mp\_5\_4\_origination}} | |

| **MP-5 (4) What is the solution and how is it implemented?** |
| --- |
| {{mp\_5\_4\_implementation}} |

MP-6 Media Sanitization and Disposal (H)

The organization:

1. Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using[*FedRAMP Assignment: techniques and procedures IAW NIST SP 800-88 R1, Appendix A - Minimum Sanitization Recommendations*] in accordance with applicable federal and organizational standards and policies; and
2. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

| **MP-6** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{mp\_6\_role}} | |
| Parameter MP-6(a)-1: {{mp\_6\_a\_1\_parameter}} | |
| Parameter MP-6(a)-2: {{mp\_6\_a\_2\_parameter}} | |
| {{mp\_6\_status}} | |
| {{mp\_6\_origination}} | |

| **MP-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{mp\_6\_a\_implementation}} |
| **Part b** | {{mp\_6\_b\_implementation}} |

MP-6 (1) Control Enhancement (H)

The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

| **MP-6 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{mp\_6\_1\_role}} | |
| {{mp\_6\_1\_status}} | |
| {{mp\_6\_1\_origination}} | |

| **MP-6 (1) What is the solution and how is it implemented?** |
| --- |
| {{mp\_6\_1\_implementation}} |

MP-6 (2) Control Enhancement (H)

The organization tests sanitization equipment and procedures [*FedRAMP Assignment: at least every six (6) months*] to verify that the intended sanitization is being achieved.

**MP-6(2) Additional FedRAMP Requirements and Guidance:**

**Guidance:** Equipment and procedures may be tested or evaluated for effectiveness.

| **MP-6 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{mp\_6\_2\_role}} | |
| Parameter MP-06(2): {{mp\_6\_2\_parameter}} | |
| {{mp\_6\_2\_status}} | |
| {{mp\_6\_2\_origination}} | |

| **MP-6 (2) What is the solution and how is it implemented?** |
| --- |
| {{mp\_6\_2\_implementation}} |

MP-6 (3) Control Enhancement (H)

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined circumstances requiring sanitization of portable storage devices*].

| **MP-6 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{mp\_6\_3\_role}} | |
| Parameter MP-6 (3): {{mp\_6\_3\_parameter}} | |
| {{mp\_6\_3\_status}} | |
| {{mp\_6\_3\_origination}} | |

| **MP-6 (3) What is the solution and how is it implemented?** |
| --- |
| {{mp\_6\_3\_implementation}} |

MP-7 Media Use (L) (M) (H)

The organization [*Selection: restricts; prohibits*] the use of [*Assignment: organization-defined types of information system media*] on [*Assignment: organization-defined information systems or system components*] using [*Assignment: organization-defined security safeguards*].

| **MP-7** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{mp\_7\_role}} | |
| Parameter MP-7-1: {{mp\_7\_1\_parameter}} | |
| Parameter MP-7-2: {{mp\_7\_2\_parameter}} | |
| Parameter MP-7-3: {{mp\_7\_3\_parameter}} | |
| Parameter MP-7-4: {{mp\_7\_4\_parameter}} | |
| {{mp\_7\_status}} | |
| {{mp\_7\_origination}} | |

| **MP-7 What is the solution and how is it implemented?** |
| --- |
| {{mp\_7\_implementation}} |

MP-7 (1) Control Enhancement (M) (H)

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

| **MP-7 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{mp\_7\_1\_role}} | |
| {{mp\_7\_1\_status}} | |
| {{mp\_7\_1\_origination}} | |

| **MP-7 (1) is the solution and how is it implemented?** |
| --- |
| {{mp\_7\_1\_implementation}} |

## Physical and Environmental Protection (PE)

PE-1 Physical and Environmental Protection Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
2. Reviews and updates the current:
   1. Physical and environmental protection policy [*FedRAMP Assignment: at least annually* ]; and
   2. Physical and environmental protection procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| **PE-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_1\_role}} | |
| Parameter PE-1(a): {{pe\_1\_a\_parameter}} | |
| Parameter PE-1(b)(1): {{pe\_1\_b\_1\_parameter}} | |
| Parameter PE-1(b)(2): {{pe\_1\_b\_2\_parameter}} | |
| {{pe\_1\_status}} | |
| {{pe\_1\_origination}} | |

| **PE-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{pe\_1\_a\_implementation}} |
| **Part b** | {{pe\_1\_b\_implementation}} |

PE-2 Physical Access Authorizations (H)

The organization:

1. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
2. Issues authorization credentials for facility access;
3. Reviews the access list detailing authorized facility access by individuals [*FedRAMP Assignment: at least every ninety (90) days* ]; and
4. Removes individuals from the facility access list when access is no longer required.

| **PE-2** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_2\_role}} | |
| Parameter PE-02(c): {{pe\_2\_c\_parameter}} | |
| {{pe\_2\_status}} | |
| {{pe\_2\_origination}} | |

| **PE-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{pe\_2\_a\_implementation}} |
| **Part b** | {{pe\_2\_b\_implementation}} |
| **Part c** | {{pe\_2\_c\_implementation}} |
| **Part d** | {{pe\_2\_d\_implementation}} |

PE-3 Physical Access Control (L) (M) (H)

The organization:

1. Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by:
   1. Verifying individual access authorizations before granting access to the facility; and
2. Controlling ingress/egress to the facility using [*FedRAMP Assignment: CSP defined physical access control systems/devices AND guards*];
3. Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*];
4. Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible;
5. Escorts visitors and monitors visitor activity [*FedRAMP Assignment: in all circumstances within restricted access area where the information system resides*];
6. Secures keys, combinations, and other physical access devices;
7. Inventories [*Assignment: organization-defined physical access devices*] every [*FedRAMP Assignment: at least annually*]; and
8. Changes combinations and keys [*FedRAMP Assignment: at least annually*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

| **PE-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_3\_role}} | |
| Parameter PE-3(a)(1): {{pe\_3\_a\_1\_parameter}} | |
| Parameter PE-3(a)(2): {{pe\_3\_a\_2\_parameter}} | |
| Parameter PE-3(b): {{pe\_3\_b\_parameter}} | |
| Parameter PE-3(c): {{pe\_3\_c\_parameter}} | |
| Parameter PE-3(d): {{pe\_3\_d\_parameter}} | |
| Parameter PE-3(f)-1: {{pe\_3\_f\_1\_parameter}} | |
| Parameter PE-3(f)-2: {{pe\_3\_f\_2\_parameter}} | |
| Parameter PE-3(g): {{pe\_3\_g\_parameter}} | |
| {{pe\_3\_status}} | |
| {{pe\_3\_origination}} | |

| **PE-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{pe\_3\_a\_implementation}} |
| **Part b** | {{pe\_3\_b\_implementation}} |
| **Part c** | {{pe\_3\_c\_implementation}} |
| **Part d** | {{pe\_3\_d\_implementation}} |
| **Part e** | {{pe\_3\_e\_implementation}} |
| **Part f** | {{pe\_3\_f\_implementation}} |
| **Part g** | {{pe\_3\_g\_implementation}} |

PE-3 (1) Control Enhancement (H)

The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [*Assignment: organization-defined physical spaces containing components of the information system*].

| **PE-3 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_3\_1\_role}} | |
| Parameter PE-3 (1): {{pe\_3\_1\_parameter}} | |
| {{pe\_3\_1\_status}} | |
| {{pe\_3\_1\_origination}} | |

| **PE-3 (1) What is the solution and how is it implemented?** |
| --- |
| {{pe\_3\_1\_implementation}} |

PE-4 Access Control for Transmission Medium (M) (H)

The organization controls physical access to [*Assignment: organization-defined information system distribution and transmission lines*] within organizational facilities using [*Assignment: organization-defined security safeguards*].

| **PE-4** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_4\_role}} | |
| Parameter PE-4-1: {{pe\_4\_1\_parameter}} | |
| Parameter PE-4-2: {{pe\_4\_2\_parameter}} | |
| {{pe\_4\_status}} | |
| {{pe\_4\_origination}} | |

| **PE-4 What is the solution and how is it implemented?** |
| --- |
| {{pe\_4\_implementation}} |

PE-5 Access Control for Output Devices (M) (H)

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

| **PE-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_5\_role}} | |
| {{pe\_5\_status}} | |
| {{pe\_5\_origination}} | |

| **PE-5 What is the solution and how is it implemented?** |
| --- |
| {{pe\_5\_implementation}} |

PE-6 Monitoring Physical Access (L) (M) (H)

The organization:

1. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
2. Reviews physical access logs [*FedRAMP Assignment: at least monthly*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; and
3. Coordinates results of reviews and investigations with the organization’s incident response capability.

| **PE-6** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_6\_role}} | |
| Parameter PE-6(b)-1: {{pe\_6\_b\_1\_parameter}} | |
| Parameter PE-6(b)-2: {{pe\_6\_b\_2\_parameter}} | |
| {{pe\_6\_status}} | |
| {{pe\_6\_origination}} | |

| **PE-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{pe\_6\_a\_implementation}} |
| **Part b** | {{pe\_6\_b\_implementation}} |
| **Part c** | {{pe\_6\_c\_implementation}} |

PE-6 (1) Control Enhancement (M) (H)

The organization monitors physical intrusion alarms and surveillance equipment.

| **PE-6 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_6\_1\_role}} | |
| {{pe\_6\_1\_status}} | |
| {{pe\_6\_1\_origination}} | |

| **PE-6 (1) What is the solution and how is it implemented?** |
| --- |
| {{pe\_6\_1\_implementation}} |

PE-6 (4) Control Enhancement (H)

The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [*Assignment: organization-defined physical spaces containing one or more components of the information system*].

| **PE-6 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_6\_4\_role}} | |
| Parameter PE-6 (4): {{pe\_6\_4\_parameter}} | |
| {{pe\_6\_4\_status}} | |
| {{pe\_6\_4\_origination}} | |

| **PE-6 (4) What is the solution and how is it implemented?** |
| --- |
| {{pe\_6\_4\_implementation}} |

PE-8 Visitor Access Records (L) (M) (H)

The organization:

1. Maintains visitor access records to the facility where the information system resides for [*FedRAMP Assignment: for a minimum of one (1) year*]; and
2. Reviews visitor access records [*FedRAMP Assignment: at least monthly*]

| **PE-8** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_8\_role}} | |
| Parameter PE-8(a): {{pe\_8\_a\_parameter}} | |
| Parameter PE-8(b): {{pe\_8\_b\_parameter}} | |
| {{pe\_8\_status}} | |
| {{pe\_8\_origination}} | |

| **PE-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{pe\_8\_a\_implementation}} |
| **Part b** | {{pe\_8\_b\_implementation}} |

PE-8 (1) Control Enhancement (H)

The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

| **PE-8 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_8\_1\_role}} | |
| {{pe\_8\_1\_status}} | |
| {{pe\_8\_1\_origination}} | |

| **PE-8 (1) What is the solution and how is it implemented?** |
| --- |
| {{pe\_8\_1\_implementation}} |

PE-9 Power Equipment and Cabling (M) (H)

The organization protects power equipment and power cabling for the information system from damage and destruction.

| **PE-9** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_9\_role}} | |
| {{pe\_9\_status}} | |
| {{pe\_9\_origination}} | |

| **PE-9 What is the solution and how is it implemented?** |
| --- |
| {{pe\_9\_implementation}} |

PE-10 Emergency Shutoff (M) (H)

The organization:

1. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
2. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and
3. Protects emergency power shutoff capability from unauthorized activation.

| **PE-10** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_10\_role}} | |
| Parameter PE-10(b): {{pe\_10\_b\_parameter}} | |
| {{pe\_10\_status}} | |
| {{pe\_10\_origination}} | |

| **PE-10 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{pe\_10\_a\_implementation}} |
| **Part b** | {{pe\_10\_b\_implementation}} |
| **Part c** | {{pe\_10\_c\_implementation}} |

PE-11 Emergency Power (M) (H)

The organization provides a short-term uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power*] in the event of a primary power source loss.

| **PE-11** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_11\_role}} | |
| Parameter PE-11: {{pe\_11\_parameter}} | |
| {{pe\_11\_status}} | |
| {{pe\_11\_origination}} | |

| **PE-11 What is the solution and how is it implemented?** |
| --- |
| {{pe\_11\_implementation}} |

PE-11 (1) Control Enhancement (H)

The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

| **PE-11 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_11\_1\_role}} | |
| {{pe\_11\_1\_status}} | |
| {{pe\_11\_1\_origination}} | |

| **PE-11 (1) What is the solution and how is it implemented?** |
| --- |
| {{pe\_11\_1\_implementation}} |

PE-12 Emergency Lighting (L) (M) (H)

The organization employs and maintains automatic emergency lighting for the information 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: {{pe\_12\_role}} | |
| {{pe\_12\_status}} | |
| {{pe\_12\_origination}} | |

| **PE-12 What is the solution and how is it implemented?** |
| --- |
| {{pe\_12\_implementation}} |

PE-13 Fire Protection (L) (M) (H)

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

| **PE-13** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_13\_role}} | |
| {{pe\_13\_status}} | |
| {{pe\_13\_origination}} | |

| **PE-13 What is the solution and how is it implemented?** |
| --- |
| {{pe\_13\_implementation}} |

PE-13 (1) Control Enhancement (H)

The organization employs fire detection devices/systems for the information system that activate automatically and notify [*FedRAMP Assignment: service provider building maintenance/physical security personnel*] and [*FedRAMP Assignment: service provider emergency responders with incident response responsibilities*] in the event of a fire.

| **PE-13 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_13\_1\_role}} | |
| Parameter PE-13 (1)-1: {{pe\_13\_1\_1\_parameter}} | |
| Parameter PE-13 (1)-2: {{pe\_13\_1\_2\_parameter}} | |
| {{pe\_13\_1\_status}} | |
| {{pe\_13\_1\_origination}} | |

| **PE-13 (1) What is the solution and how is it implemented?** |
| --- |
| {{pe\_13\_1\_implementation}} |

PE-13 (2) Control Enhancement (M) (H)

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*].

| **PE-13 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_13\_2\_role}} | |
| Parameter PE-13(2)-1: {{pe\_13\_2\_1\_parameter}} | |
| Parameter PE-13(2)-2: {{pe\_13\_2\_2\_parameter}} | |
| {{pe\_13\_2\_status}} | |
| {{pe\_13\_2\_origination}} | |

| **PE-13 (2) What is the solution and how is it implemented?** |
| --- |
| {{pe\_13\_2\_implementation}} |

PE-13 (3) Control Enhancement (M) (H)

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

| **PE-13 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_13\_3\_role}} | |
| {{pe\_13\_3\_status}} | |
| {{pe\_13\_3\_origination}} | |

| **PE-13 (3) What is the solution and how is it implemented?** |
| --- |
| {{pe\_13\_3\_implementation}} |

PE-14 Temperature and Humidity Controls (L) (M) (H)

The organization:

1. Maintains temperature and humidity levels within the facility where the information system resides at [*FedRAMP Assignment: consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled "Thermal Guidelines for Data Processing Environments*]; and

**PE-14 (a) Additional FedRAMP Requirements and Guidance:   
Requirement:** *The service provider measures temperature at server inlets and humidity levels by dew point*.

1. Monitors temperature and humidity levels [*FedRAMP Assignment: continuously*].

| **PE-14** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_14\_role}} | |
| Parameter PE-14(a): {{pe\_14\_a\_parameter}} | |
| Parameter PE-14(b): {{pe\_14\_b\_parameter}} | |
| {{pe\_14\_status}} | |
| {{pe\_14\_origination}} | |
| Responsible Role: {{pe\_14\_role}} | |

| **PE-14 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{pe\_14\_a\_implementation}} |
| **Part b** | {{pe\_14\_b\_implementation}} |

PE-14 (2) Control Enhancement (M) (H)

The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

| **PE-14 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_14\_2\_role}} | |
| {{pe\_14\_2\_status}} | |
| {{pe\_14\_2\_origination}} | |

| **PE-14 (2) What is the solution and how is it implemented?** |
| --- |
| {{pe\_14\_2\_implementation}} |

PE-15 Water Damage Protection (L) (M) (H)

The organization protects the information 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: {{pe\_15\_role}} | |
| {{pe\_15\_status}} | |
| {{pe\_15\_origination}} | |

| **PE-15 What is the solution and how is it implemented?** |
| --- |
| {{pe\_15\_implementation}} |

PE-15 (1) Control Enhancement (H)

The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [*FedRAMP Assignment: service provider building maintenance /physical security personnel*].

| **PE-15 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_15\_1\_role}} | |
| Parameter PE-15 (1): {{pe\_15\_1\_parameter}} | |
| {{pe\_15\_1\_status}} | |
| {{pe\_15\_1\_origination}} | |

| **PE-15 (1) What is the solution and how is it implemented?** |
| --- |
| {{pe\_15\_1\_implementation}} |

PE-16 Delivery and Removal (L) (M) (H)

The organization authorizes, monitors, and controls [*FedRAMP Assignment: all information system components*] entering and exiting the facility and maintains records of those items.

| **PE-16** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_16\_role}} | |
| Parameter PE-16: {{pe\_16\_parameter}} | |
| {{pe\_16\_status}} | |
| {{pe\_16\_origination}} | |

| **PE-16 What is the solution and how is it implemented?** |
| --- |
| {{pe\_16\_implementation}} |

PE-17 Alternate Work Site (M) (H)

The organization:

1. Employs [*Assignment: organization-defined security controls*] at alternate work sites*;*
2. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
3. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

| **PE-17** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_17\_role}} | |
| Parameter PE-17(a): {{pe\_17\_a\_parameter}} | |
| {{pe\_17\_status}} | |
| {{pe\_17\_origination}} | |

| **PE-17 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{pe\_17\_a\_implementation}} |
| **Part b** | {{pe\_17\_b\_implementation}} |
| **Part c** | {{pe\_17\_c\_implementation}} |

PE-18 Location of Information System Components (H)

The organization positions information system components within the facility to minimize potential damage from [*FedRAMP Assignment: physical and environmental hazards identified during threat assessment*] and to minimize the opportunity for unauthorized access.

| **PE-18** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pe\_18\_role}} | |
| Parameter PE-18: {{pe\_18\_parameter}} | |
| {{pe\_18\_status}} | |
| {{pe\_18\_origination}} | |

| **PE-18 What is the solution and how is it implemented?** |
| --- |
| {{pe\_18\_implementation}} |

## Planning (PL)

PL-1 Security Planning Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
2. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
4. Reviews and updates the current:
5. Security planning policy [*FedRAMP Assignment: at least annually*]; and
6. Security planning procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| **PL-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pl\_1\_role}} | |
| Parameter PL-01(a): {{pl\_1\_a\_parameter}} | |
| Parameter PL-1(b)(1): {{pl\_1\_b\_1\_parameter}} | |
| Parameter PL-1(b)(2): {{pl\_1\_b\_2\_parameter}} | |
| {{pl\_1\_status}} | |
| {{pl\_1\_origination}} | |

| **PL-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{pl\_1\_a\_implementation}} |
| **Part b** | {{pl\_1\_b\_implementation}} |

PL-2 System Security Plan (L) (M) (H)

The organization:

1. Develops a security plan for the information system that:
2. Is consistent with the organization’s enterprise architecture;
3. Explicitly defines the authorization boundary for the system;
4. Describes the operational context of the information system in terms of missions and business processes;
5. Provides the security categorization of the information system including supporting rationale;
6. Describes the operational environment for the information system and relationships with or connections to other information;
7. Provides an overview of the security requirements for the system;
8. Identifies any relevant overlays, if applicable;
9. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
10. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
11. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*];
12. Reviews the security plan for the information system [*FedRAMP Assignment: at least annually*];
13. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
14. Protects the security plan from unauthorized disclosure and modification.

| **PL-2** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pl\_2\_role}} | |
| Parameter PL-02(b): {{pl\_2\_b\_parameter}} | |
| Parameter PL-2(c): {{pl\_2\_c\_parameter}} | |
| {{pl\_2\_status}} | |
| {{pl\_2\_origination}} | |

| **PL-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{pl\_2\_a\_implementation}} |
| **Part b** | {{pl\_2\_b\_implementation}} |
| **Part c** | {{pl\_2\_c\_implementation}} |
| **Part d** | {{pl\_2\_d\_implementation}} |
| **Part e** | {{pl\_2\_e\_implementation}} |

PL-2 (3) Control Enhancement (M) (H)

The organization plans and coordinates security-related activities affecting the information system with [*Assignment: organization-defined individuals or groups*] before conducting such activities in order to reduce the impact on other organizational entities.

| **PL-2 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pl\_2\_3\_role}} | |
| Parameter PL-2(3): {{pl\_2\_3\_parameter}} | |
| {{pl\_2\_3\_status}} | |
| {{pl\_2\_3\_origination}} | |

| **PL-2 (3) What is the solution and how is it implemented?** |
| --- |
| {{pl\_2\_3\_implementation}} |

PL-4 Rules of Behavior (H)

The organization:

1. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
2. Receives a signed 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 information system;
3. Reviews and updates the rules of behavior [*FedRAMP Assignment: annually*]; and
4. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

| **PL-4** | | **Control Summary Information** |
| --- | --- | --- |
| Responsible Role: {{pl\_4\_role}} | | |
| Parameter PL-04(c): {{pl\_4\_parameter}} | | |
| {{pl\_4\_status}} | | |
| {{pl\_4\_origination}} | | |
| **PL-4 What is the solution and how is it implemented?** | | |
| **Part a** | {{pl\_4\_a\_implementation}} | |
| **Part b** | {{pl\_4\_b\_implementation}} | |
| **Part c** | {{pl\_4\_c\_implementation}} | |
| **Part d** | {{pl\_4\_d\_implementation}} | |

PL-4 (1) Control Enhancement (M) (H)

The organization includes in the rules of behavior, explicit restrictions on the use of social media/ networking sites and posting organizational information on public websites.

| **PL-4 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pl\_4\_1\_role}} | |
| {{pl\_4\_1\_status}} | |
| {{pl\_4\_1\_origination}} | |

| **PL-4 (1) What is the solution and how is it implemented?** |
| --- |
| {{pl\_4\_1\_implementation}} |

PL-8 Information Security Architecture (M) (H)

The organization:

1. Develops an information security architecture for the information system that:
   1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
   2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
   3. Describes any information security assumptions about, and dependencies on, external services;
2. Reviews and updates the information security architecture [*FedRAMP Assignment: at least annually or when a significant change occurs*] to reflect updates in the enterprise architecture; and

**PL-8 (b) Additional FedRAMP Requirements and Guidance:**

**Guidance:** Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F, on Page F-8.

1. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

| **PL-8** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{pl\_8\_role}} | |
| Parameter PL-8(b): {{pl\_8\_b\_parameter}} | |
| {{pl\_8\_status}} | |
| {{pl\_8\_origination}} | |

| **PL-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{pl\_8\_a\_implementation}} |
| **Part b** | {{pl\_8\_b\_implementation}} |
| **Part c** | {{pl\_8\_c\_implementation}} |

## Personnel Security (PS)

PS-1 Personnel Security Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
2. Reviews and updates the current:
   1. Personnel security policy [*FedRAMP Assignment: at least annually*]; and
   2. Personnel security procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| **PS-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ps\_1\_role}} | |
| Parameter PS-01(a): {{ps\_1\_a\_parameter}} | |
| Parameter PS-01(b)(1): {{ps\_1\_b\_1\_parameter}} | |
| Parameter PS-1(b)(2): {{ps\_1\_b\_2\_parameter}} | |
| {{ps\_1\_status}} | |
| {{ps\_1\_origination}} | |

| **PS-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ps\_1\_a\_implementation}} |
| **Part b** | {{ps\_1\_b\_implementation}} |

PS-2 Position Categorization (H)

The organization:

1. Assigns a risk designation to all positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and revises position risk designations [*FedRAMP* *Assignment: at least annually*].

| **PS-2** | | **Control Summary Information** |
| --- | --- | --- |
| Responsible Role: {{ps\_2\_role}} | | |
| Parameter PS-2(c): {{ps\_2\_c\_parameter}} | | |
| {{ps\_2\_status}} | | |
| {{ps\_2\_origination}} | | |
| **PS-2 What is the solution and how is it implemented?** | | |
| **Part a** | {{ps\_2\_a\_implementation}} | |
| **Part b** | {{ps\_2\_b\_implementation}} | |
| **Part c** | {{ps\_2\_c\_implementation}} | |

PS-3 Personnel Screening (L) (M) (H)

The organization:

1. Screens individuals prior to authorizing access to the information system; and
2. Rescreens individuals according to [*FedRAMP* *Assignment: For national security clearances; a reinvestigation is required during the fifth (5th) year for top secret security clearance, the tenth (10th) year for secret security clearance, and fifteenth (15th) year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth (5th) year. There is no reinvestigation for other moderate risk positions or any low risk positions*].

| **PS-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ps\_3\_role}} | |
| Parameter PS-03(b): {{ps\_3\_b\_parameter}} | |
| {{ps\_3\_status}} | |
| {{ps\_3\_origination}} | |

| **PS-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ps\_3\_a\_implementation}} |
| **Part b** | {{ps\_3\_b\_implementation}} |

PS-3 (3) Control Enhancement (M) (H)

The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

1. Have valid access authorizations that are demonstrated by assigned official government duties; and
2. Satisfy [*FedRAMP Assignment: personnel screening criteria – as required by specific information*].

| **PS-3 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ps\_3\_3\_role}} | |
| Parameter PS-3(3)(b): {{ps\_3\_3\_b\_parameter}} | |
| {{ps\_3\_3\_status}} | |
| {{ps\_3\_3\_origination}} | |

| **PS-3 (3) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ps\_3\_3\_a\_implementation}} |
| **Part b** | {{ps\_3\_3\_b\_implementation}} |

PS-4 Personnel Termination (H)

The organization, upon termination of individual employment:

1. Disables information system access within [*FedRAMP Assignment: eight (8) hours*];
2. Terminates/revokes any authenticators/credentials associated with the individual;
3. Conducts exit interviews that include a discussion of [*Assignment: organization-defined information security topics*];
4. Retrieves all security-related organizational information system-related property;
5. Retains access to organizational information and information systems formerly controlled by terminated individual; and
6. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].

| **PS-4** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ps\_4\_role}} | |
| Parameter PS-04(a): {{ps\_4\_a\_parameter}} | |
| Parameter PS-4(c): {{ps\_4\_c\_parameter}} | |
| Parameter PS-4(f)-1: {{ps\_4\_f\_1\_parameter}} | |
| Parameter PS-4(f)-2: {{ps\_4\_f\_2\_parameter}} | |
| {{ps\_4\_status}} | |
| {{ps\_4\_origination}} | |

| **PS-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ps\_4\_a\_implementation}} |
| **Part b** | {{ps\_4\_b\_implementation}} |
| **Part c** | {{ps\_4\_c\_implementation}} |
| **Part d** | {{ps\_4\_d\_implementation}} |
| **Part e** | {{ps\_4\_e\_implementation}} |
| **Part f** | {{ps\_4\_f\_implementation}} |

PS-4 (2) Control Enhancement (H)

The organization employs automated mechanisms to notify [*FedRAMP Assignment: access control personnel responsible for disabling access to the system*] upon termination of an individual.

| **PS-4 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ps\_4\_2\_role}} | |
| Parameter PS-4 (2): {{ps\_4\_2\_parameter}} | |
| {{ps\_4\_2\_status}} | |
| {{ps\_4\_2\_origination}} | |

| **PS-4 (2) What is the solution and how is it implemented?** |
| --- |
| {{ps\_4\_2\_implementation}} |

PS-5 Personnel Transfer (H)

The organization:

1. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
2. Initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*FedRAMP Assignment: twenty-four (24) hours*];
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies [*Assignment: organization-defined personnel or roles*] within [*FedRAMP Assignment: twenty-four (24) hours*].

| **PS-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ps\_5\_role}} | |
| Parameter PS-5(b)-1: {{ps\_5\_b\_1\_parameter}} | |
| Parameter PS-5(b)-2: {{ps\_5\_b\_2\_parameter}} | |
| Parameter PS-5(d)-1: {{ps\_5\_d\_1\_parameter}} | |
| Parameter PS-5(d)-2: {{ps\_5\_d\_2\_parameter}} | |
| {{ps\_5\_status}} | |
| {{ps\_5\_origination}} | |

| **PS-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ps\_5\_a\_implementation}} |
| **Part b** | {{ps\_5\_b\_implementation}} |
| **Part c** | {{ps\_5\_c\_implementation}} |
| **Part d** | {{ps\_5\_d\_implementation}} |

PS-6 Access Agreements (H)

The organization:

1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements [*FedRAMP Assignment: at least annually*]; and
3. Ensures that individuals requiring access to organizational information and information systems:
   1. Sign appropriate access agreements prior to being granted access; and
   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [*FedRAMP Assignment: at least annually and any time there is a change to the user's level of access*]

| **PS-6** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ps\_6\_role}} | |
| Parameter PS-6(b): {{ps\_6\_b\_parameter}} | |
| Parameter PS-6(c)(2): {{ps\_6\_c\_2\_parameter}} | |
| {{ps\_6\_status}} | |
| {{ps\_6\_origination}} | |

| **PS-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ps\_6\_a\_implementation}} |
| **Part b** | {{ps\_6\_b\_implementation}} |
| **Part c** | {{ps\_6\_c\_implementation}} |

PS-7 Third-Party Personnel Security (H)

The organization:

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
3. Documents personnel security requirements;
4. Requires third-party providers to notify [*Assignment: organization-defined personnel or roles*]of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [*FedRAMP Assignment: terminations: immediately; transfers: within twenty-four (24) hours*]; and
5. Monitors provider compliance.

| **PS-7** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ps\_7\_role}} | |
| Parameter PS-07(d)-1: {{ps\_7\_d\_1\_parameter}} | |
| Parameter PS-7(d)-2: {{ps\_7\_d\_2\_parameter}} | |
| {{ps\_7\_status}} | |
| {{ps\_7\_origination}} | |

| **PS-7 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ps\_7\_a\_implementation}} |
| **Part b** | {{ps\_7\_b\_implementation}} |
| **Part c** | {{ps\_7\_c\_implementation}} |
| **Part d** | {{ps\_7\_d\_implementation}} |
| **Part e** | {{ps\_7\_e\_implementation}} |

PS-8 Personnel Sanctions (H)

The organization:

1. Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
2. Notifies [*FedRAMP Assignment: at a minimum, the ISSO and/or similar role within the organization*]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: {{ps\_8\_role}} | |
| Parameter PS-8(b)-1: {{ps\_8\_b\_1\_parameter}} | |
| Parameter PS-8(b)-2: {{ps\_8\_b\_2\_parameter}} | |
| {{ps\_8\_status}} | |
| {{ps\_8\_origination}} | |

| **PS-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ps\_8\_a\_implementation}} |
| **Part b** | {{ps\_8\_b\_implementation}} |

## Risk Assessment (RA)

RA-1 Risk Assessment Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
2. Reviews and updates the current:
   1. Risk assessment policy [*FedRAMP Assignment: at least annually*]; and
   2. Risk assessment procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| **RA-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ra\_1\_role}} | |
| Parameter RA-01(a): {{ra\_1\_a\_parameter}} | |
| Parameter RA-01(b)(1): {{ra\_1\_b\_1\_parameter}} | |
| Parameter RA-1(b)(2): {{ra\_1\_b\_2\_parameter}} | |
| {{ps\_1\_status}} | |
| {{ra\_1\_origination}} | |

| **RA-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ra\_1\_a\_implementation}} |
| **Part b** | {{ra\_1\_b\_implementation}} |

RA-2 Security Categorization (L) (M) (H)

The organization:

1. Categorizes information and the information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
3. Ensures the security categorization decision is reviewed and approved by the AO or authorizing official designated representative.

| **RA-2** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ra\_2\_role}} | |
| {{ra\_2\_status}} | |
| {{ra\_2\_origination}} | |

| **RA-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ra\_2\_a\_implementation}} |
| **Part b** | {{ra\_2\_b\_implementation}} |
| **Part c** | {{ra\_2\_c\_implementation}} |

RA-3 Risk Assessment (H)

The organization:

1. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
2. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*FedRAMP Assignment: security assessment report*];
3. Reviews risk assessment results [*FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs*];
4. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and
5. Updates the risk assessment [*FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs]*; or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

**RA-3 Additional FedRAMP Requirements and Guidance:**

**Guidance:** Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F

**RA-3 (d) Requirement:** Include all Authorizing Officials; for JAB authorizations to include FedRAMP.

| **RA-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ra\_3\_role}} | |
| Parameter RA-03(b): {{ra\_3\_b\_parameter}} | |
| Parameter RA-03(c): {{ra\_3\_c\_parameter}} | |
| Parameter RA-03(d): {{ra\_3\_d\_parameter}} | |
| Parameter RA-3(e): {{ra\_3\_e\_parameter}} | |
| {{ra\_3\_status}} | |
| {{ra\_3\_origination}} | |

| **RA-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ra\_3\_a\_implementation}} |
| **Part b** | {{ra\_3\_b\_implementation}} |
| **Part c** | {{ra\_3\_c\_implementation}} |
| **Part d** | {{ra\_3\_d\_implementation}} |
| **Part e** | {{ra\_3\_e\_implementation}} |

RA-5 Vulnerability Scanning (L) (M) (H)

The organization:

1. Scans for vulnerabilities in the information system and hosted applications [*FedRAMP Assignment: monthly operating system/infrastructure; monthly web applications and databases*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

**RA-5 (a) Additional FedRAMP Requirements and Guidance:**

**Requirement:** An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.

1. Employs vulnerability scanning tools and techniques that promote 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 and making transparent, checklists and test procedures; and
   3. Measuring vulnerability impact;
2. Analyzes vulnerability scan reports and results from security control assessments
3. Remediates legitimate vulnerabilities; [*FedRAMP Assignment: high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery*], in accordance with an organizational assessment of risk; and
4. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

**RA-5 (e) Additional FedRAMP Requirements and Guidance:**

**Requirement:** To include all Authorizing Officials; for JAB authorizations to include FedRAMP.

**RA-5 Additional FedRAMP Requirements and Guidance**

**Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Vulnerability Scanning Requirements**

| **RA-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ra\_5\_role}} | |
| Parameter RA-5(a): {{ra\_5\_a\_parameter}} | |
| Parameter RA-5(d): {{ra\_5\_d\_parameter}} | |
| Parameter RA-5(e): {{ra\_5\_e\_parameter}} | |
| {{ra\_5\_status}} | |
| {{ra\_5\_origination}} | |

| **RA-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{ra\_5\_a\_implementation}} |
| **Part b** | {{ra\_5\_b\_implementation}} |
| **Part c** | {{ra\_5\_c\_implementation}} |
| **Part d** | {{ra\_5\_d\_implementation}} |
| **Part e** | {{ra\_5\_e\_implementation}} |

RA-5 (1) Control Enhancement (M) (H)

The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities to be scanned.

| **RA-5 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ra\_5\_1\_role}} | |
| {{ra\_5\_1\_status}} | |
| {{ra\_5\_1\_origination}} | |

| **RA-5 (1) What is the solution and how is it implemented?** |
| --- |
| {{ra\_5\_1\_implementation}} |

RA-5 (2) Control Enhancement (M) (H)

The organization updates the information system vulnerabilities scanned [*Selection (one or more):* [*FedRAMP* *Assignment: prior to a new scan*]].

| **RA-5 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ra\_5\_2\_role}} | |
| Parameter RA-5(2): {{ra\_5\_2\_parameter}} | |
| {{ra\_5\_2\_status}} | |
| {{ra\_5\_2\_origination}} | |

| **RA-5 (2) What is the solution and how is it implemented?** |
| --- |
| {{ra\_5\_2\_implementation}} |

RA-5 (3) Control Enhancement (M) (H)

The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

| **RA-5 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ra\_5\_3\_role}} | |
| {{ra\_5\_3\_status}} | |
| {{ra\_5\_3\_origination}} | |

| **RA-5 (3) What is the solution and how is it implemented?** |
| --- |
| {{ra\_5\_3\_implementation}} |

RA-5 (4) Control Enhancement (H)

The organization determines what information about the information system is discoverable by adversaries and subsequently takes [*FedRAMP Assignment: notify appropriate service provider personnel and follow procedures for organization and service provider-defined corrective actions*].

| **RA-5 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ra\_5\_4\_role}} | |
| Parameter RA-5 (4): {{ra\_5\_4\_parameter}} | |
| {{ra\_5\_4\_status}} | |
| {{ra\_5\_4\_origination}} | |

| **RA-5 (4) What is the solution and how is it implemented?** |
| --- |
| {{ra\_5\_4\_implementation}} |

RA-5 (5) Control Enhancement (M) (H)

The organization includes privileged access authorization to [*FedRAMP Assignment: operating systems, databases, web applications*] for selected [*FedRAMP Assignment: all scans*].

| **RA-5 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ra\_5\_5\_role}} | |
| Parameter RA-5(5)-1: {{ra\_5\_5\_1\_parameter}} | |
| Parameter RA-5(5)-2: {{ra\_5\_5\_2\_parameter}} | |
| {{ra\_5\_5\_status}} | |
| {{ra\_5\_5\_origination}} | |

| **RA-5 (5) What is the solution and how is it implemented?** |
| --- |
| {{ra\_5\_5\_implementation}} |

RA-5 (6) Control Enhancement (M) (H)

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

| **RA-5 (6)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ra\_5\_6\_role}} | |
| {{ra\_5\_6\_status}} | |
| {{ra\_5\_6\_origination}} | |

| **RA-5 (6) What is the solution and how is it implemented?** |
| --- |
| {{ra\_5\_6\_implementation}} |

RA-5 (8) Control Enhancement (L) (M) (H)

The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

**RA-5(8) Additional FedRAMP Requirements and Guidance:**

**Requirement:** This enhancement is required for all high vulnerability scan findings.

**Guidance:** While scanning tools may label findings as high or critical, the intent of the control is based around NIST's definition of high vulnerability.

| **RA-5 (8)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ra\_5\_8\_role}} | |
| {{ra\_5\_8\_status}} | |
| {{ra\_5\_8\_origination}} | |

| **RA-5 (8) What is the solution and how is it implemented?** |
| --- |
| {{ra\_5\_8\_implementation}} |

RA-5 (10) Control Enhancement (H)

The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.

**RA-5 (10) Additional FedRAMP Requirements and Guidance:**

**Guidance:** If multiple tools are not used, this control is not applicable.

| **RA-5 (10)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{ra\_5\_10\_role}} | |
| {{ra\_5\_10\_status}} | |
| {{ra\_5\_10\_origination}} | |

| **RA-5 (10) What is the solution and how is it implemented?** |
| --- |
| {{ra\_5\_10\_implementation}} |

## System and Services Acquisition (SA)

SA-1 System and Services Acquisition Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
2. Reviews and updates the current:
   1. System and services acquisition policy [*FedRAMP Assignment: at least annually*]; and
   2. System and services acquisition procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| **SA-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_1\_role}} | |
| Parameter SA-1(a): {{sa\_1\_a\_parameter}} | |
| Parameter SA-1(b)(1): {{sa\_1\_b\_1\_parameter}} | |
| Parameter SA-1(b)(2): {{sa\_1\_b\_2\_parameter}} | |
| {{sa\_1\_status}} | |
| {{sa\_1\_origination}} | |

| **SA-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sa\_1\_a\_implementation}} |
| **Part b** | {{sa\_1\_b\_implementation}} |

SA-2 Allocation of Resources (L) (M) (H)

The organization:

1. Determines information security requirements for the information system or information system service in mission/business process planning;
2. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
3. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

| **SA-2** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_2\_role}} | |
| {{sa\_2\_status}} | |
| {{sa\_2\_origination}} | |

| **SA-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sa\_2\_a\_implementation}} |
| **Part b** | {{sa\_2\_b\_implementation}} |
| **Part c** | {{sa\_2\_c\_implementation}} |

SA-3 System Development Life Cycle (L) (M) (H)

The organization:

1. Manages the information system using [*Assignment: organization-defined system development life cycle*] that incorporates information security considerations;
2. Defines and documents information security roles and responsibilities throughout the system development life cycle;
3. Identifies individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into system development life cycle activities.

| **SA-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_3\_role}} | |
| Parameter SA-3(a): {{sa\_3\_a\_parameter}} | |
| {{sa\_3\_status}} | |
| {{sa\_3\_origination}} | |

| **SA-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sa\_3\_a\_implementation}} |
| **Part b** | {{sa\_3\_b\_implementation}} |
| **Part c** | {{sa\_3\_c\_implementation}} |
| **Part d** | {{sa\_3\_d\_implementation}} |

SA-4 Acquisitions Process (L) (M) (H)

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

1. Security functional requirements;
2. Security strength requirements;
3. Security assurance requirements;
4. Security-related documentation requirements;
5. Requirements for protecting security-related documentation;
6. Description of the information system development environment and environment in which the system is intended to operate; and
7. Acceptance criteria.

**Additional FedRAMP Requirements and Guidance:**

**Guidance**: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.  
See <https://www.niap-ccevs.org/Product/PCL.cfm> or [http://www.commoncriteriaportal.org/products](http://www.commoncriteriaportal.org/products.html)

| **SA-4** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_4\_role}} | |
| {{sa\_4\_status}} | |
| {{sa\_4\_origination}} | |

| **SA-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sa\_4\_a\_implementation}} |
| **Part b** | {{sa\_4\_b\_implementation}} |
| **Part c** | {{sa\_4\_c\_implementation}} |
| **Part d** | {{sa\_4\_d\_implementation}} |
| **Part e** | {{sa\_4\_e\_implementation}} |
| **Part f** | {{sa\_4\_f\_implementation}} |
| **Part g** | {{sa\_4\_g\_implementation}} |

SA-4 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

| **SA-4 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_4\_1\_role}} | |
| {{sa\_4\_1\_status}} | |
| {{sa\_4\_1\_origination}} | |

| **SA-4 (1) What is the solution and how is it implemented?** |
| --- |
| {{sa\_4\_1\_implementation}} |

SA-4 (2) Control Enhancement (H)

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*FedRAMP Selection (one or more): at a minimum to include security-relevant external system interfaces; high-level design; low-level design; source code or network and data flow diagram*]*; [organization-defined design/implementation information]]*at [*Assignment: organization-defined level of detail*].

| **SA-4 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_4\_2\_role}} | |
| Parameter SA-4(2)-1: {{sa\_4\_2\_1\_parameter}} | |
| Parameter SA-4(2)-2: {{sa\_4\_2\_2\_parameter}} | |
| {{sa\_4\_2\_status}} | |
| {{sa\_4\_2\_origination}} | |
| **SA-4 (2) What is the solution and how is it implemented?** | |
| {{sa\_4\_2\_implementation}} | |

SA-4 (8) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [*FedRAMP Assignment: at least the minimum requirement as defined in control CA-7*].

**SA-4 (8) Additional FedRAMP Requirements and Guidance:**

**Guidance:** CSP must use the same security standards regardless of where the system component or information system service is acquired.

| **SA-4 (8)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_4\_8\_role}} | |
| Parameter SA-4(8): {{sa\_4\_8\_parameter}} | |
| {{sa\_4\_8\_status}} | |
| {{sa\_4\_8\_origination}} | |

| **SA-4 (8) What is the solution and how is it implemented?** |
| --- |
| {{sa\_4\_8\_implementation}} |

SA-4 (9) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

| **SA-4 (9)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_4\_9\_role}} | |
| {{sa\_4\_9\_status}} | |
| {{sa\_4\_9\_origination}} | |

| **SA-4 (9) What is the solution and how is it implemented?** |
| --- |
| {{sa\_4\_9\_implementation}} |

SA-4 (10) Control Enhancement (M) (H)

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

| **SA-4 (10)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_4\_10\_role}} | |
| {{sa\_4\_10\_status}} | |
| {{sa\_4\_10\_origination}} | |

| **SA-4 (10) What is the solution and how is it implemented?** |
| --- |
| {{sa\_4\_10\_implementation}} |

SA-5 Information System Documentation (H)

The organization:

1. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
2. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;
3. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [*Assignment: organization-defined actions*] in response;
4. Protects documentation as required, in accordance with the risk management strategy; and
5. Distributes documentation to [*FedRAMP Assignment: at a minimum, the ISSO (or similar role within the organization]*.

| **SA-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_5\_role}} | |
| Parameter SA-5(c): {{sa\_5\_c\_parameter}} | |
| Parameter SA-5(e): {{sa\_5\_e\_parameter}} | |
| {{sa\_5\_status}} | |
| {{sa\_5\_origination}} | |

| **SA-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sa\_5\_a\_implementation}} |
| **Part b** | {{sa\_5\_b\_implementation}} |
| **Part c** | {{sa\_5\_c\_implementation}} |
| **Part d** | {{sa\_5\_d\_implementation}} |
| **Part e** | {{sa\_5\_e\_implementation}} |

SA-8 Security Engineering Principles (M) (H)

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

| **SA-8** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_8\_role}} | |
| {{sa\_8\_status}} | |
| {{sa\_8\_origination}} | |

| **SA-8 What is the solution and how is it implemented?** |
| --- |
| {{sa\_8\_implementation}} |

SA-9 External Information System Services (L) (M) (H)

The organization:

1. Requires that providers of external information system services comply with organizational information security requirements and employ [*FedRAMP Assignment: FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
3. Employs [*FedRAMP Assignment: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored*] to monitor security control compliance by external service providers on an ongoing basis.

**Additional FedRAMP Requirements and Guidance**

**Guidance:** See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Continuous Monitoring Strategy Guide  
<https://www.fedramp.gov/documents>

**Guidance**: Independent Assessors should assess the risk associated with the use of external services. See the FedRAMP page under Key Cloud Service Provider (CSP) Documents>FedRAMP Authorization Boundary Guidance

| **SA-9** | | **Control Summary Information** |
| --- | --- | --- |
| Responsible Role: {{sa\_9\_role}} | | |
| Parameter SA-09(a): {{sa\_9\_a\_parameter}} | | |
| Parameter SA-9(c): {{sa\_9\_c\_parameter}} | | |
| {{sa\_9\_status}} | | |
| {{sa\_9\_origination}} | | |
| **SA-9 What is the solution and how is it implemented?** | | |
| **Part a** | {{sa\_9\_a\_implementation}} | |
| **Part b** | {{sa\_9\_b\_implementation}} | |
| **Part c** | {{sa\_9\_c\_implementation}} | |

SA-9 (1) Control Enhancement (M) (H)

The organization:

1. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and
2. Ensures 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: {{sa\_9\_1\_role}} | |
| Parameter SA-9(1)(b): {{sa\_9\_1\_1\_b\_parameter}} | |
| {{sa\_9\_1\_status}} | |
| {{sa\_9\_1\_origination}} | |

| **SA-9 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sa\_9\_1\_a\_implementation}} |
| **Part b** | {{sa\_9\_1\_b\_implementation}} |

**SA-9 (1) Additional FedRAMP Requirements and Guidance:**

**Requirement**: The service provider documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. For JAB authorizations, future planned outsourced services are approved and accepted by the JAB.

| SA-9 (1) Req. | Control Summary Information |
| --- | --- |
| Responsible Role: {{sa\_9\_1\_r\_role}} | |
| {{sa\_9\_1\_r\_status}} | |
| {{sa\_9\_1\_r\_origination}} | |

| SA-09 (1) Additional - What is the solution and how is it implemented? |
| --- |
| {{sa\_9\_1\_r\_implementation}} |

SA-9 (2) Control Enhancement (M) (H)

The organization requires providers of [*FedRAMP Assignment: All external systems where Federal information is processed or stored*] to identify the functions, ports, protocols, and other services required for the use of such services.

| **SA-9 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_9\_2\_role}} | |
| Parameter SA-9(2): {{sa\_9\_2\_parameter}} | |
| {{sa\_9\_2\_status}} | |
| {{sa\_9\_2\_origination}} | |

| **SA-9 (2) What is the solution and how is it implemented?** |
| --- |
| {{sa\_9\_2\_implementation}}. |

SA-9 (4) Control Enhancement (M) (H)

The organization employs [*Assignment: organization-defined security safeguards*] to ensure that the interests of [*FedRAMP Assignment: All external systems where Federal information is processed or stored*] are consistent with and reflect organizational interests.

| **SA-9 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_9\_4\_role}} | |
| Parameter SA-9(4)-1: {{sa\_9\_4\_1\_parameter}} | |
| Parameter SA-9(4)-2: {{sa\_9\_4\_2\_parameter}} | |
| {{sa\_9\_4\_status}} | |
| {{sa\_9\_4\_origination}} | |

| **SA-9 (4) What is the solution and how is it implemented?** |
| --- |
| {{sa\_9\_4\_implementation}} |

SA-9 (5) Control Enhancement (M) (H)

The organization restricts the location of [*FedRAMP Selection: information processing, information data, AND information services*] to [*Assignment: organization-defined locations*] based on [*Assignment: organization-defined requirements or conditions*].

**Additional FedRAMP Requirements and Guidance**

**Guidance**: System services refer to FTP, Telnet, and TFTP, etc.

| **SA-9 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_9\_5\_role}} | |
| Parameter SA-9(5)-1: {{sa\_9\_5\_1\_parameter}} | |
| Parameter SA-9(5)-2: {{sa\_9\_5\_2\_parameter}} | |
| Parameter SA-9(5)-3: {{sa\_9\_5\_3\_parameter}} | |
| {{sa\_9\_5\_status}} | |
| {{sa\_9\_5\_origination}} | |

| **SA-9 (5) What is the solution and how is it implemented?** |
| --- |
| {{sa\_9\_5\_implementation}} |

SA-10 Developer Configuration Management (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

1. Perform configuration management during system, component, or service [*FedRAMP Selection: development, implementation, AND operation*];
2. Document, manage, and control the integrity of changes to [*Assignment: organization-defined configuration items under configuration management*];
3. Implement only organization-approved changes to the system, component, or service;
4. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
5. Track security flaws and flaw resolution within the system, component, or service and report findings to [*Assignment: organization-defined personnel*].

**SA-10 (e) Additional FedRAMP Requirements and Guidance:**

**Requirement:** For JAB authorizations, track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP.

| **SA-10** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_10\_role}} | |
| Parameter SA-10(a): {{sa\_10\_a\_parameter}} | |
| Parameter SA-10(b): {{sa\_10\_b\_parameter}} | |
| Parameter SA-10(e): {{sa\_10\_e\_parameter}} | |
| {{sa\_10\_status}} | |
| {{sa\_10\_origination}} | |

| **SA-10 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sa\_10\_a\_implementation}} |
| **Part b** | {{sa\_10\_b\_implementation}} |
| **Part c** | {{sa\_10\_c\_implementation}} |
| **Part d** | {{sa\_10\_d\_implementation}} |
| **Part e** | {{sa\_10\_e\_implementation}} |

SA-10 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

| **SA-10 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_10\_1\_role}} | |
| {{sa\_10\_1\_status}} | |
| {{sa\_10\_1\_origination}} | |

| **SA-10 (1) What is the solution and how is it implemented?** |
| --- |
| {{sa\_10\_1\_implementation}} |

SA-11 Developer Security Testing and Evaluation (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

1. Create and implement a security assessment plan;
2. Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation at [*Assignment: organization-defined depth and coverage*];
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
4. Implement a verifiable flaw remediation process; and
5. Correct flaws identified during security testing/evaluation.

| **SA-11** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_11\_role}} | |
| Parameter SA-11(b)-1: {{sa\_11\_b\_1\_parameter}} | |
| Parameter SA-11(b)-2: {{sa\_11\_b\_2\_parameter}} | |
| {{sa\_11\_status}} | |
| {{sa\_11\_origination}} | |

| **SA-11 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sa\_11\_a\_implementation}} |
| **Part b** | {{sa\_11\_b\_implementation}} |
| **Part c** | {{sa\_11\_c\_implementation}} |
| **Part d** | {{sa\_11\_d\_implementation}} |
| **Part e** | {{sa\_11\_e\_implementation}} |

SA-11 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

**SA-11 (1) Additional FedRAMP Requirements and Guidance:**

**Requirement:** The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

| **SA-11 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_11\_1\_role}} | |
| {{sa\_11\_1\_status}} | |
| {{sa\_11\_1\_origination}} | |

| **SA-11 (1) What is the solution and how is it implemented?** |
| --- |
| {{sa\_11\_1\_implementation}} |

SA-11 (2) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/ evaluation of the as-built system, component, or service.

| **SA-11 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_11\_2\_role}} | |
| {{sa\_11\_2\_status}} | |
| {{sa\_11\_2\_origination}} | |

| **SA-11 (2) What is the solution and how is it implemented?** |
| --- |
| {{sa\_11\_2\_implementation}} |

SA-11 (8) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

| **SA-11 (8)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_11\_8\_role}} | |
| {{sa\_11\_8\_status}} | |
| {{sa\_11\_8\_origination}} | |

| **SA-11 (8) What is the solution and how is it implemented?** |
| --- |
| {{sa\_11\_8\_implementation}} |

SA-12 Supply Chain Protection (H)

The organization protects against supply chain threats to the information system, system component, or information system service by employing [*FedRAMP Assignment: organization and service provider-defined personnel security requirements, approved HW/SW vendor list/ process, and secure SDLC procedures*] as part of a comprehensive, defense-in-breadth information security strategy.

| **SA-12** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_12\_role}} | |
| Parameter SA-12: {{sa\_12\_parameter}} | |
| {{sa\_12\_status}} | |
| {{sa\_12\_origination}} | |

| **SA-12 What is the solution and how is it implemented?** |
| --- |
| {{sa\_12\_implementation}} |

SA-15 Development Process, Standards, and Tools (H)

The organization:

1. Requires the developer of the information system, system component, or information system service to follow a documented development process that:
   1. Explicitly addresses security 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
2. Reviews the development process, standards, tools, and tool options/configurations [*FedRAMP* *Assignment: as needed and as dictated by the current threat posture*] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [*FedRAMP* *Assignment: organization and service provider- defined security requirements*].

| **SA-15** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_15\_role}} | |
| Parameter SA-15 (b)-1: {{sa\_15\_b\_1\_parameter}} | |
| Parameter SA-15 (b)-2: {{sa\_15\_b\_2\_parameter}} | |
| {{sa\_15\_status}} | |
| {{sa\_15\_origination}} | |

| **SA-15 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sa\_15\_a\_implementation}} |
| **Part b** | {{sa\_15\_b\_implementation}} |

SA-16 Developer-Provided Training (H)

The organization requires the developer of the information system, system component, or information system service to provide [*Assignment: organization-defined training*] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

| **SA-16** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_16\_role}} | |
| Parameter SA-16: {{sa\_16\_parameter}} | |
| {{sa\_16\_status}} | |
| {{sa\_16\_origination}} | |

| **SA-16 What is the solution and how is it implemented?** |
| --- |
| {{sa\_16\_implementation}} |

SA-17 Developer Security Architecture and Design (H)

The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

1. Is consistent with and supportive of the organization’s security architecture which is established within and is an integrated part of the organization’s enterprise architecture;
2. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
3. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

| **SA-17** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sa\_17\_role}} | |
| {{sa\_17\_status}} | |
| {{sa\_17\_origination}} | |

| **SA-17 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sa\_17\_a\_implementation}} |
| **Part b** | {{sa\_17\_b\_implementation}} |
| **Part c** | {{sa\_17\_c\_implementation}} |

## System and Communications Protection (SC)

SC-1 System and Communications Protection Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
2. Reviews and updates the current:
   1. System and communications protection policy [*FedRAMP* *Assignment: at least annually*]; and
   2. System and communications protection procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| **SC-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_1\_role}} | |
| Parameter SC-1(a): {{sc\_1\_a\_parameter}} | |
| Parameter SC-1(b)(1): {{sc\_1\_b\_1\_parameter}} | |
| Parameter SC-1(b)(2): {{sc\_1\_b\_2\_parameter}} | |
| {{sc\_1\_status}} | |
| {{sc\_1\_origination}} | |

| **SC-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sc\_1\_a\_implementation}} |
| **Part b** | {{sc\_1\_b\_implementation}} |

SC-2 Application Partitioning (M) (H)

The information system separates user functionality (including user interface services) from information system management functionality.

| **SC-2** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_2\_role}} | |
| {{sc\_2\_status}} | |
| {{sc\_2\_origination}} | |

| **SC-2 What is the solution and how is it implemented?** |
| --- |
| {{sc\_2\_implementation}} |

SC-3 Security Function Isolation (H)

The information system isolates security functions from non-security functions.

| **SC-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_3\_role}} | |
| {{sc\_3\_status}} | |
| {{sc\_3\_origination}} | |

| **SC-3 What is the solution and how is it implemented?** |
| --- |
| {{sc\_3\_implementation}} |

SC-4 Information in Shared Resources (M) (H)

The information system prevents unauthorized and unintended information transfer via shared system resources.

| **SC-4** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_4\_role}} | |
| {{sc\_4\_status}} | |
| {{sc\_4\_origination}} | |

| **SC-4 What is the solution and how is it implemented?** |
| --- |
| {{sc\_4\_implementation}} |

SC-5 Denial of Service Protection (L) (M) (H)

The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined types of denial of service attacks or reference to source for such information*] by employing [*Assignment: organization-defined security safeguards*].

| **SC-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_5\_role}} | |
| Parameter SC-5-1: {{sc\_5\_1\_parameter}} | |
| Parameter SC-5-2: {{sc\_5\_2\_parameter}} | |
| {{sc\_5\_status}} | |
| {{sc\_5\_origination}} | |

| **SC-5 What is the solution and how is it implemented?** |
| --- |
| {{sc\_5\_implementation}} |

SC-6 Resource Availability (M) (H)

The information system protects the availability of resources by allocating [*Assignment: organization-defined resources*] by [*Selection (one or more); priority; quota;* [*Assignment: organization-defined security safeguards*]].

| **SC-6** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_6\_role}} | |
| Parameter SC-6-1: {{sc\_6\_1\_parameter}} | |
| Parameter SC-6-2: {{sc\_6\_2\_parameter}} | |
| Parameter SC-6-3: {{sc\_6\_3\_parameter}} | |
| {{sc\_6\_status}} | |
| {{sc\_6\_origination}} | |

| **SC-6 What is the solution and how is it implemented?** |
| --- |
| {{sc\_6\_implementation}} |

SC-7 Boundary Protection (L) (M) (H)

The information system:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
2. Implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and
3. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

| **SC-7** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_7\_role}} | |
| Parameter SC-07(b): {{sc\_7\_b\_parameter}} | |
| {{sc\_7\_status}} | |
| {{sc\_7\_origination}} | |

| **SC-7 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sc\_7\_a\_implementation}} |
| **Part b** | {{sc\_7\_b\_implementation}} |
| **Part c** | {{sc\_7\_c\_implementation}} |

SC-7 (3) Control Enhancement (M) (H)

The organization limits the number external network connections to the information system.

| **SC-7 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_7\_3\_role}} | |
| {{sc\_7\_3\_status}} | |
| {{sc\_7\_3\_origination}} | |

| **SC-7 (3) What is the solution and how is it implemented?** |
| --- |
| {{sc\_7\_3\_implementation}} |

SC-7 (4) Control Enhancement (H)

The organization:

1. Implements a managed interface for each external telecommunication service;
2. Establishes a traffic flow policy for each managed interface;
3. Protects the confidentiality and integrity of the information being transmitted across each interface;
4. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
5. Reviews exceptions to the traffic flow policy [*FedRAMP Assignment: at least every ninety (90) days or whenever there is a change in the threat environment that warrants a review of the exceptions*] and removes exceptions that are no longer supported by an explicit mission/business need.

| **SC-7 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_7\_4\_role}} | |
| Parameter SC-07(4)(e): {{sc\_7\_4\_e\_parameter}} | |
| {{sc\_7\_4\_status}} | |
| {{sc\_7\_4\_origination}} | |

| **SC-7 (4) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sc\_7\_4\_a\_implementation}} |
| **Part b** | {{sc\_7\_4\_b\_implementation}} |
| **Part c** | {{sc\_7\_4\_c\_implementation}} |
| **Part d** | {{sc\_7\_4\_d\_implementation}} |
| **Part e** | {{sc\_7\_4\_e\_implementation}} |

SC-7 (5) Control Enhancement (M) (H)

The information system at managed interfaces denies network traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

| **SC-7 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_7\_5\_role}} | |
| {{sc\_7\_5\_status}} | |
| {{sc\_7\_5\_origination}} | |

| **SC-7 (5) What is the solution and how is it implemented?** |
| --- |
| {{sc\_7\_5\_implementation}} |

SC-7 (7) Control Enhancement (M) (H)

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

| **SC-7 (7)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_7\_7\_role}} | |
| {{sc\_7\_7\_status}} | |
| {{sc\_7\_7\_origination}} | |

| **SC-7 (7) What is the solution and how is it implemented?** |
| --- |
| {{sc\_7\_7\_implementation}} |

SC-7 (8) Control Enhancement (M) (H)

The information system routes [*Assignment: organization-defined internal communications traffic*] through authenticated proxy servers at managed interfaces.

| **SC-7 (8)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_7\_8\_role}} | |
| Parameter SC-7(8)-1: {{sc\_7\_8\_1\_parameter}} | |
| Parameter SC-7(8)-2: {{sc\_7\_8\_2\_parameter}} | |
| {{sc\_7\_8\_status}} | |
| {{sc\_7\_8\_origination}} | |

| **SC-7 (8) What is the solution and how is it implemented?** |
| --- |
| {{sc\_7\_8\_implementation}} |

SC-7 (10) Control Enhancement (H)

The organization prevents the unauthorized exfiltration of information across managed interfaces.

| **SC-7 (10)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_7\_10\_role}} | |
| {{sc\_7\_10\_status}} | |
| {{sc\_7\_10\_origination}} | |

| **SC-7 (10) What is the solution and how is it implemented?** |
| --- |
| {{sc\_7\_10\_implementation}} |

SC-7 (12) Control Enhancement (H)

The organization implements [*FedRAMP Assignment: Host Intrusion Prevention System (HIPS), Host Intrusion Detection System (HIDS), or minimally a host-based firewall*] at [*Assignment: organization-defined information system components*].

| **SC-7 (12)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_7\_12\_role}} | |
| Parameter SC-7(12)-1: {{sc\_7\_12\_1\_parameter}} | |
| Parameter SC-7(12)-2: {{sc\_7\_12\_2\_parameter}} | |
| {{sc\_7\_12\_status}} | |
| {{sc\_7\_12\_origination}} | |

| **SC-7 (12) What is the solution and how is it implemented?** |
| --- |
| {{sc\_7\_12\_implementation}} |

SC-7 (13) Control Enhancement (H)

The organization isolates [*FedRAMP* *Assignment: See SC-7 (13) additional FedRAMP Requirements and Guidance*] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

**SC-7 (13) Additional FedRAMP Requirements and Guidance:**

**Requirement**: The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

**Guidance**: Examples include: information security tools, mechanisms, and support components such as, but not limited to public key infrastructure (PKI), patching infrastructure, cyber defense tools, special purpose gateway, vulnerability tracking systems, internet access points (IAPs); network element and data center administrative/management traffic; demilitarized zones (DMZs), Server farms/computing centers, centralized audit log servers, etc.

| **SC-7 (13)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_7\_13\_role}} | |
| Parameter SC-07(13): {{sc\_7\_13\_parameter}} | |
| {{sc\_7\_13\_status}} | |
| {{sc\_7\_13\_origination}} | |

| **SC-7 (13) What is the solution and how is it implemented?** |
| --- |
| {{sc\_7\_13\_implementation}} |

SC-7 (18) Control Enhancement (M) (H)

The information system fails securely in the event of an operational failure of a boundary protection device.

| **SC-7 (18)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_7\_18\_role}} | |
| {{sc\_7\_18\_status}} | |
| {{sc\_7\_18\_origination}} | |

| **SC-7 (18) What is the solution and how is it implemented?** |
| --- |
| {{sc\_7\_18\_implementation}} |

SC-7 (20) Control Enhancement (H)

The information system provides the capability to dynamically isolate/segregate [*Assignment: organization-defined information system components*] from other components of the system.

| **SC-7 (20)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_7\_20\_role}} | |
| Parameter SC-7(20): {{sc\_7\_20\_parameter}} | |
| {{sc\_7\_20\_status}} | |
| {{sc\_7\_20\_origination}} | |

| **SC-7 (20) What is the solution and how is it implemented?** |
| --- |
| {{sc\_7\_20\_implementation}} |

SC-7 (21) Control Enhancement (H)

The organization employs boundary protection mechanisms to separate [*Assignment: organization-defined information system components*] supporting [*Assignment: organization-defined mission and/or business functions*].

| **SC-7 (21)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_7\_21\_role}} | |
| Parameter SC-7 (21)-1: {{sc\_7\_21\_1\_parameter}} | |
| Parameter SC-7 (21)-2: {{sc\_7\_21\_2\_parameter}} | |
| {{sc\_7\_21\_status}} | |
| {{sc\_7\_21\_origination}} | |

| **SC-7 (21) What is the solution and how is it implemented?** |
| --- |
| {{sc\_7\_21\_implementation}} |

SC-8 Transmission confidentiality and Integrity (M) (H)

The information system protects the [*FedRAMP Assignment: confidentiality AND integrity*] of transmitted information.

| **SC-8** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_8\_role}} | |
| Parameter SC-8: {{sc\_8\_parameter}} | |
| {{sc\_8\_status}} | |
| {{sc\_8\_origination}} | |

| **SC-8 What is the solution and how is it implemented?** |
| --- |
| {{sc\_8\_implementation}} |

SC-8 (1) Control Enhancement (M) (H)

The information system implements cryptographic mechanisms to [*FedRAMP Assignment: prevent unauthorized disclosure of information AND detect changes to information*] during transmission unless otherwise protected by [*FedRAMP Assignment: a hardened or alarmed carrier Protective Distribution System (PDS)*].

| **SC-8 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_8\_1\_role}} | |
| Parameter SC-8(1)-1: {{sc\_8\_1\_1\_parameter}} | |
| Parameter SC-8(1)-2: {{sc\_8\_1\_2\_parameter}} | |
| {{sc\_8\_1\_status}} | |
| {{sc\_8\_1\_origination}} | |

| **SC-8 (1) What is the solution and how is it implemented?** |
| --- |
| {{sc\_8\_1\_implementation}} |

SC-10 Network Disconnect (H)

The information system terminates the network connection associated with a communications session at the end of the session or after [*FedRAMP Assignment: no longer than ten (10) minutes for privileged sessions and no longer than fifteen (15) minutes for user session*] of inactivity.

| **SC-10** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_10\_role}} | |
| Parameter SC-10: {{sc\_10\_parameter}} | |
| {{sc\_10\_status}} | |
| {{sc\_10\_origination}} | |

| **SC-10 What is the solution and how is it implemented?** |
| --- |
| {{sc\_10\_implementation}} |

SC-12 Cryptographic Key Establishment & Management (L) (M) (H)

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

| **SC-12** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_12\_role}} | |
| Parameter SC-12: {{sc\_12\_parameter}} | |
| {{sc\_12\_status}} | |
| {{sc\_12\_origination}} | |

| **SC-12 What is the solution and how is it implemented?** |
| --- |
| {{sc\_12\_implementation}} |

SC-12 (1) Control Enhancement (H)

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

| **SC-12 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_12\_1\_role}} | |
| {{sc\_12\_1\_status}} | |
| {{sc\_12\_1\_origination}} | |

| **SC-12 (1) What is the solution and how is it implemented?** |
| --- |
| {{sc\_12\_1\_implementation}} |

SC-12 (2) Control Enhancement (M) (H)

The organization produces, controls, and distributes symmetric cryptographic keys using [*FedRAMP* *Selection: NIST FIPS-compliant*] key management technology and processes.

| **SC-12 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_12\_2\_role}} | |
| Parameter SC-12(2): {{sc\_12\_2\_parameter}} | |
| {{sc\_12\_2\_status}} | |
| {{sc\_12\_2\_origination}} | |

| **SC-12 (2) What is the solution and how is it implemented?** |
| --- |
| {{sc\_12\_2\_implementation}} |

SC-12 (3) Control Enhancement (M) (H)

The organization produces, controls, and distributes asymmetric cryptographic keys using [*Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key*].

| **SC-12 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_12\_3\_role}} | |
| Parameter SC-12 (3): {{sc\_12\_3\_parameter}} | |
| {{sc\_12\_3\_status}} | |
| {{sc\_12\_3\_origination}} | |

| **SC-12 (3) What is the solution and how is it implemented?** |
| --- |
| {{sc\_12\_3\_implementation}} |

SC-13 Use of Cryptography (L) (M) (H)

The information system implements [*FedRAMP Assignment:* *FIPS-validated or NSA-approved cryptography]* in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

| **SC-13** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_13\_role}} | |
| Parameter SC-13: {{sc\_13\_parameter}} | |
| {{sc\_13\_status}} | |
| {{sc\_13\_origination}} | |

| **SC-13 What is the solution and how is it implemented?** |
| --- |
| {{sc\_13\_implementation}} |

SC-15 Collaborative Computing Devices (M) (H)

The information system:

1. Prohibits remote activation of collaborative computing devices with the following exceptions: [*FedRAMP Assignment: no exceptions*] and
2. Provides an explicit indication of use to users physically present at the devices.

**SC-15 Additional FedRAMP Requirements and Guidance:**

**Requirement:** The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

| **SC-15** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_15\_role}} | |
| Parameter SC-15(a): {{sc\_15\_a\_parameter}} | |
| {{sc\_15\_status}} | |
| {{sc\_15\_origination}} | |

| **SC-15 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sc\_15\_a\_implementation}} |
| **Part b** | {{sc\_15\_b\_implementation}} |

**SC-15 Additional FedRAMP Requirements and Guidance:**

**Requirement**: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

| **SC-15 Req.** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_15\_r\_role}} | |
| {{sc\_15\_r\_status}} | |
| {{sc\_15\_r\_origination}} | |

| **SC-15 What is the solution and how is it implemented?** | |
| --- | --- |
| **Req. 1** | {{sc\_15\_r\_implementation}} |

SC-17 Public Key Infrastructure Certificates (M) (H)

The organization issues public key certificates under an [*Assignment: organization-defined certificate policy*]or obtains public key certificates from an approved service provider.

| **SC-17** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_17\_role}} | |
| Parameter SC-17: {{sc\_17\_parameter}} | |
| {{sc\_17\_status}} | |
| {{sc\_17\_origination}} | |

| **SC-17 What is the solution and how is it implemented?** |
| --- |
| {{sc\_17\_implementation}} |

SC-18 Mobile Code (M) (H)

The organization:

1. Defines acceptable and unacceptable mobile code and mobile code technologies;
2. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
3. Authorizes, monitors, and controls the use of mobile code within the information system.

| **SC-18** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_18\_role}} | |
| {{sc\_18\_status}} | |
| {{sc\_18\_origination}} | |

| **SC-18 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sc\_18\_a\_implementation}} |
| **Part b** | {{sc\_18\_b\_implementation}} |
| **Part c** | {{sc\_18\_c\_implementation}} |

SC-19 Voice Over Internet Protocol (M) (H)

The organization:

1. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
2. Authorizes, monitors, and controls the use of VoIP within the information system.

| **SC-19** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_19\_role}} | |
| {{sc\_19\_status}} | |
| {{sc\_19\_origination}} | |

| **SC-19 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sc\_19\_a\_implementation}} |
| **Part b** | {{sc\_19\_b\_implementation}} |

SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H)

The information system:

1. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

| **SC-20** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_20\_role}} | |
| {{sc\_20\_status}} | |
| {{sc\_20\_origination}} | |

| **SC-20 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{sc\_20\_a\_implementation}} |
| **Part b** | {{sc\_20\_b\_implementation}} |

SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H)

The information system requests and performs 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: {{sc\_21\_role}} | |
| {{sc\_21\_status}} | |
| {{sc\_21\_origination}} | |

| **SC-21 What is the solution and how is it implemented?** |
| --- |
| {{sc\_21\_implementation}} |

SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H)

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

| **SC-22** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_22\_role}} | |
| {{sc\_22\_status}} | |
| {{sc\_22\_origination}} | |

| **SC-22 What is the solution and how is it implemented?** |
| --- |
| {{sc\_22\_implementation}} |

SC-23 Session Authenticity (M) (H)

The information system protects the authenticity of communications sessions.

| **SC-23** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_23\_role}} | |
| {{sc\_23\_status}} | |
| {{sc\_23\_origination}} | |

| **SC-23 What is the solution and how is it implemented?** |
| --- |
| {{sc\_23\_implementation}} |

SC-23 (1) Enhancement (H)

The information system invalidates session identifiers upon user logout or other session termination.

| **SC-23 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_23\_1\_role}} | |
| {{sc\_23\_1\_status}} | |
| {{sc\_23\_1\_origination}} | |

| **SC-23 (1) What is the solution and how is it implemented?** |
| --- |
| {{sc\_23\_1\_implementation}} |

SC-24 Fail in Known State (H)

The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.

| **SC-24** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_24\_role}} | |
| Parameter SC-24-1: {{sc\_24\_1\_parameter}} | |
| Parameter SC-24-2: {{sc\_24\_2\_parameter}} | |
| Parameter SC-24-3: {{sc\_24\_3\_parameter}} | |
| {{sc\_24\_status}} | |
| {{sc\_24\_origination}} | |

| **SC-24 What is the solution and how is it implemented?** |
| --- |
| {{sc\_24\_implementation}} |

SC-28 Protection of Information at Rest (M) (H)

The information system protects the [*FedRAMP* *Selection: confidentiality AND integrity*] of [*Assignment: organization-defined information at rest*].

**SC-28 Additional FedRAMP Requirements and Guidance:**

**Guidance:** The organization supports the capability to use cryptographic mechanisms to protect information at rest.

| **SC-28** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_28\_role}} | |
| Parameter SC-28-1: {{sc\_28\_1\_parameter}} | |
| Parameter SC-28-2: {{sc\_28\_2\_parameter}} | |
| {{sc\_28\_status}} | |
| {{sc\_28\_origination}} | |

| **SC-28 What is the solution and how is it implemented?** |
| --- |
| {{sc\_28\_implementation}} |

SC-28 (1) Control Enhancement (M) (H)

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*FedRAMP Assignment: all information system components storing customer data deemed sensitive*]

| **SC-28 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_28\_1\_role}} | |
| Parameter SC-28(1)-1: {{sc\_28\_1\_1\_parameter}} | |
| Parameter SC-28(1)-2: {{sc\_28\_1\_2\_parameter}} | |
| {{sc\_28\_1\_status}} | |
| {{sc\_28\_1\_origination}} | |

| **SC-28 (1) What is the solution and how is it implemented?** |
| --- |
| {{sc\_28\_1\_implementation}} |

SC-39 Process Isolation (L) (M) (H)

The information system maintains a separate execution domain for each executing process.

| **SC-39** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{sc\_39\_role}} | |
| {{sc\_39\_status}} | |
| {{sc\_39\_origination}} | |

| **SC-39 What is the solution and how is it implemented?** |
| --- |
| {{sc\_39\_implementation}} |

## System and Information Integrity (SI)

SI-1 System and Information Integrity Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
2. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
4. Reviews and updates the current:
5. System and information integrity policy [*FedRAMP Assignment: at least annually*]; and
6. System and information integrity procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| **SI-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_1\_role}} | |
| Parameter SI-1(a): {{si\_1\_a\_parameter}} | |
| Parameter SI-1(b)(1): {{si\_1\_b\_1\_parameter}} | |
| Parameter SI-1(b)(2): {{si\_1\_b\_2\_parameter}} | |
| {{si\_1\_status}} | |
| {{si\_1\_origination}} | |

| **SI-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{si\_1\_a\_implementation}} |
| **Part b** | {{si\_1\_b\_implementation}} |

SI-2 Flaw Remediation (L) (M) (H)

The organization:

1. Identifies, reports, and corrects information system flaws;
2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Installs security-relevant software and firmware updates within [*FedRAMP Assignment: thirty (30) days of release of updates*] of the release of the updates; and
4. Incorporates flaw remediation into the organizational configuration management process.

| **SI-2** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_2\_role}} | |
| Parameter SI-2(c): {{si\_2\_c\_parameter}} | |
| {{si\_2\_status}} | |
| {{si\_2\_origination}} | |

| **SI-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{si\_2\_a\_implementation}} |
| **Part b** | {{si\_2\_b\_implementation}} |
| **Part c** | {{si\_2\_c\_implementation}} |
| **Part d** | {{si\_2\_d\_implementation}} |

SI-2 (1) Control Enhancement (H)

The organization centrally manages the flaw remediation process.

| **SI-2 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_2\_1\_role}} | |
| {{si\_2\_1\_status}} | |
| {{si\_2\_1\_origination}} | |

| **SI-2 (1) What is the solution and how is it implemented?** |
| --- |
| {{si\_2\_1\_implementation}} |

SI-2 (2) Control Enhancement (M) (H)

The organization employs automated mechanisms [*FedRAMP Assignment: at least monthly*] to determine the state of information system components with regard to flaw remediation.

| **SI-2 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_2\_2\_role}} | |
| Parameter SI-2(2): {{si\_2\_2\_parameter}} | |
| {{si\_2\_2\_status}} | |
| {{si\_2\_2\_origination}} | |
| **SI-2 (2) What is the solution and how is it implemented?** | |
| {{si\_2\_2\_implementation}} | |

SI-2 (3) Control Enhancement (M) (H)

The organization:

1. Measures the time between flaw identification and flaw remediation; and
2. Establishes [*Assignment: organization-defined benchmarks*] for taking corrective actions.

| **SI-2 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_2\_3\_role}} | |
| Parameter SI-2(3)(b): {{si\_2\_3\_b\_parameter}} | |
| {{si\_2\_3\_status}} | |
| {{si\_2\_3\_origination}} | |

| **SI-2 (3) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{si\_2\_3\_a\_implementation}} |
| **Part b** | {{si\_2\_3\_b\_implementation}} |

SI-3 Malicious Code Protection (H)

The organization:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
   1. Perform periodic scans of the information system [*FedRAMP Assignment: at least weekly*] and real-time scans of files from external sources at [*FedRAMP Assignment: to include endpoints*] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   2. [*FedRAMP Assignment: to include blocking and quarantining malicious code and alerting administrator or defined security personnel near-real-time*] in response to malicious code detection; and
4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

| **SI-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_3\_role}} | |
| Parameter SI-3(c)(1)-1: {{si\_3\_c\_1\_1\_parameter}} | |
| Parameter SI-3(c)(1)-2: {{si\_3\_c\_1\_2\_parameter}} | |
| Parameter SI-3(c)(2): {{si\_3\_c\_2\_parameter}} | |
| {{si\_3\_status}} | |
| {{si\_3\_origination}} | |

| **SI-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{si\_3\_a\_implementation}} |
| **Part b** | {{si\_3\_b\_implementation}} |
| **Part c** | {{si\_3\_c\_implementation}} |
| **Part d** | {{si\_3\_d\_implementation}} |

SI-3 (1) Control Enhancement (M) (H)

The organization centrally manages malicious code protection mechanisms.

| **SI-3 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_3\_1\_role}} | |
| {{si\_3\_1\_status}} | |
| {{si\_3\_1\_origination}} | |

| **SI-3 (1) What is the solution and how is it implemented?** |
| --- |
| {{si\_3\_1\_implementation}} |

SI-3 (2) Control Enhancement (M) (H)

The information system automatically updates malicious code protection mechanisms.

| **SI-3 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_3\_2\_role}} | |
| {{si\_3\_2\_status}} | |
| {{si\_3\_2\_origination}} | |

| **SI-3 (2) What is the solution and how is it implemented?** |
| --- |
| {{si\_3\_2\_implementation}} |

SI-3 (7) Control Enhancement (M) (H)

The information system implements non-signature-based malicious code detection mechanisms.

| **SI-3 (7)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_3\_7\_role}} | |
| {{si\_3\_7\_status}} | |
| {{si\_3\_7\_origination}} | |

| **SI-3 (7) What is the solution and how is it implemented?** |
| --- |
| {{si\_3\_7\_implementation}} |

SI-4 Information System Monitoring (L) (M) (H)

The organization:

1. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and
   2. Unauthorized local, network, and remote connections;
2. Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];
3. Deploys monitoring devices (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
5. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
6. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
7. Provides [*Assignment: organization-defined information system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed;* [*Assignment: organization-defined frequency*]].

**SI-4 Additional FedRAMP Requirements and Guidance:**

**Guidance**: See US-CERT Incident Response Reporting Guidelines.

| **SI-4** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_role}} | |
| Parameter SI-4(a)(1): {{si\_4\_a\_1\_parameter}} | |
| Parameter SI-4(b): {{si\_4\_b\_parameter}} | |
| Parameter SI-4(g)-1: {{si\_4\_g\_1\_parameter}} | |
| Parameter SI-4(g)-2: {{si\_4\_g\_2\_parameter}} | |
| Parameter SI-4(g)-3: {{si\_4\_g\_3\_parameter}} | |
| {{si\_4\_status}} | |
| {{si\_4\_origination}} | |

| **SI-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{si\_4\_a\_implementation}} |
| **Part b** | {{si\_4\_b\_implementation}} |
| **Part c** | {{si\_4\_c\_implementation}} |
| **Part d** | {{si\_4\_d\_implementation}} |
| **Part e** | {{si\_4\_e\_implementation}} |
| **Part f** | {{si\_4\_f\_implementation}} |
| **Part g** | {{si\_4\_g\_implementation}} |

SI-4 (1) Control Enhancement (M) (H)

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

| **SI-4 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_1\_role}} | |
| {{si\_4\_1\_status}} | |
| {{si\_4\_1\_origination}} | |

| **SI-4 (1) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_1\_implementation}} |

SI-4 (2) Control Enhancement (M) (H)

The organization employs automated tools to support near real-time analysis of events.

| **SI-4 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_2\_role}} | |
| {{si\_4\_2\_status}} | |
| {{si\_4\_2\_origination}} | |

| **SI-4 (2) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_2\_implementation}} |

SI-4 (4) Control Enhancement (M) (H)

The information system monitors inbound and outbound communications traffic [*FedRAMP Assignment:* *continuously]* for unusual or unauthorized activities or conditions.

| **SI-4 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_4\_role}} | |
| Parameter SI-4(4): {{si\_4\_4\_parameter}} | |
| {{si\_4\_4\_status}} | |
| {{si\_4\_4\_origination}} | |

| **SI-4 (4) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_4\_implementation}} |

SI-4 (5) Control Enhancement (M) (H)

The information system alerts [*Assignment: organization-defined personnel or roles*] when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined compromise indicators*].

**SI-4 (5) Additional FedRAMP Requirements and Guidance:**

**Guidance**: In accordance with the incident response plan.

| **SI-4 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_5\_role}} | |
| Parameter SI-4(5)-1: {{si\_4\_5\_1\_parameter}} | |
| Parameter SI-4(5)-2: {{si\_4\_5\_2\_parameter}} | |
| {{si\_4\_5\_status}} | |
| {{si\_4\_5\_origination}} | |

| **SI-4 (5) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_5\_implementation}} |

SI-4 (11) Control Enhancement (H)

The organization analyzes outbound communications traffic at the external boundary of the information system and selected [*Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)*] to discover anomalies.

| **SI-4 (11)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_11\_role}} | |
| Parameter SI-4 (11): {{si\_4\_11\_parameter}} | |
| {{si\_4\_11\_status}} | |
| {{si\_4\_11\_origination}} | |

| **SI-4 (11) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_11\_implementation}} |

SI-4 (14) Control Enhancement (M) (H)

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

| **SI-4 (14)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_14\_role}} | |
| {{si\_4\_14\_status}} | |
| {{si\_4\_14\_origination}} | |

| **SI-4 (14) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_14\_implementation}} |

SI-4 (16) Control Enhancement (M) (H)

The organization correlates information from monitoring tools employed throughout the information system.

| **SI-4 (16)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_16\_role}} | |
| {{si\_4\_16\_status}} | |
| {{si\_4\_16\_origination}} | |

| **SI-4 (16) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_16\_implementation}} |

SI-4 (18) Control Enhancement (H)

The organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at [*Assignment: organization-defined interior points within the system* (*e.g., subnetworks, subsystems*)] to detect covert exfiltration of information.

| **SI-4 (18)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_18\_role}} | |
| Parameter SI-4 (18): {{si\_4\_18\_parameter}} | |
| {{si\_4\_18\_status}} | |
| {{si\_4\_18\_origination}} | |

| **SI-4 (18) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_18\_implementation}} |

SI-4 (19) Control Enhancement (H)

The organization implements [*Assignment: organization-defined additional monitoring*] of individuals who have been identified by [*Assignment: organization-defined sources*] as posing an increased level of risk.

| **SI-4 (19)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_19\_role}} | |
| Parameter SI-4 (19)-1: {{si\_4\_19\_1\_parameter}} | |
| Parameter SI-4 (19)-2: {{si\_4\_19\_1\_parameter}} | |
| {{si\_4\_19\_status}} | |
| {{si\_4\_19\_origination}} | |

| **SI-4 (19) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_19\_implementation}} |

SI-4 (20) Control Enhancement (H)

The organization implements [*Assignment: organization-defined additional monitoring*] of privileged users.

| **SI-4 (20)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_20\_role}} | |
| Parameter SI-4 (20): {{si\_4\_20\_parameter}} | |
| {{si\_4\_20\_status}} | |
| {{si\_4\_20\_origination}} | |

| **SI-4 (20) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_20\_implementation}} |

SI-4 (22) Control Enhancement (H)

The information system detects network services that have not been authorized or approved by [*Assignment: organization-defined authorization or approval processes*] and [*Selection (one or more): audits; alerts* [*Assignment: organization-defined personnel or roles*].

| **SI-4 (22)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_22\_role}} | |
| Parameter SI-4 (22)-1: {{si\_4\_22\_1\_parameter}} | |
| Parameter SI-4 (22)-2: {{si\_4\_22\_2\_parameter}} | |
| {{si\_4\_22\_status}} | |
| {{si\_4\_22\_origination}} | |

| **SI-4 (22) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_22\_implementation}} |

SI-4 (23) Control Enhancement (M) (H)

The organization implements [*Assignment: organization-defined host-based monitoring mechanisms*] at [*Assignment: organization-defined information system components*].

| **SI-4 (23)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_23\_role}} | |
| Parameter SI-4(23)-1: {{si\_4\_23\_1\_parameter}} | |
| Parameter SI-4(23)-2: {{si\_4\_23\_2\_parameter}} | |
| {{si\_4\_23\_status}} | |
| {{si\_4\_23\_origination}} | |

| **SI-4 (23) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_23\_implementation}} |

SI-4 (24) Control Enhancement (H)

The information system discovers, collects, distributes, and uses indicators of compromise.

| **SI-4 (24)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_4\_24\_role}} | |
| {{si\_4\_24\_status}} | |
| {{si\_4\_24\_origination}} | |

| **SI-4 (24) What is the solution and how is it implemented?** |
| --- |
| {{si\_4\_24\_implementation}} |

SI-5 Security Alerts & Advisories (L) (M) (H)

The organization:

1. Receives information system security alerts, advisories, and directives from [*FedRAMP Assignment: to include US-CERT*] on an ongoing basis;
2. Generates internal security alerts, advisories, and directives as deemed necessary;
3. Disseminates security alerts, advisories, and directives to [*FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities*]; and
4. Implements security directives in accordance with established time frames or notifies the issuing organization of the degree of noncompliance.

| **SI-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_5\_role}} | |
| Parameter SI-5(a): {{si\_5\_a\_parameter}} | |
| Parameter SI-5(c): {{si\_5\_c\_parameter}} | |
| {{si\_5\_status}} | |
| {{si\_5\_origination}} | |

| **SI-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{si\_5\_a\_implementation}} |
| **Part b** | {{si\_5\_b\_implementation}} |
| **Part c** | {{si\_5\_c\_implementation}} |
| **Part d** | {{si\_5\_d\_implementation}} |

SI-5 (1) Control Enhancement (H)

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

| **SI-5 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_5\_1\_role}} | |
| {{si\_5\_1\_status}} | |
| {{si\_5\_1\_origination}} | |

| **SI-5 (1) What is the solution and how is it implemented?** |
| --- |
| {{si\_5\_1\_implementation}} |

SI-6 Security Functionality Verification (M) (H)

The information system:

1. Verifies the correct operation of [*Assignment: organization-defined security functions*];
2. Performs this verification [*FedRAMP Assignment: to include upon system startup and/or restart at least monthly*];
3. Notifies [*FedRAMP Assignment: to include system administrators and security personnel*] of failed security verification tests; and
4. [*Selection (one or more): shuts the information system down; restarts the information system;* [*FedRAMP Assignment: to include notification of system administrators and security personnel*] when anomalies are discovered.

| **SI-6** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_6\_role}} | |
| Parameter SI-6(a): {{si\_6\_a\_parameter}} | |
| Parameter SI-6(b): {{si\_6\_b\_parameter}} | |
| Parameter SI-6(c): {{si\_6\_c\_parameter}} | |
| Parameter SI-6(d): {{si\_6\_d\_parameter}} | |
| {{si\_6\_status}} | |
| {{si\_6\_origination}} | |

| **SI-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{si\_6\_a\_implementation}} |
| **Part b** | {{si\_6\_b\_implementation}} |
| **Part c** | {{si\_6\_c\_implementation}} |
| **Part d** | {{si\_6\_d\_implementation}} |

SI-7 Software & Information Integrity (M) (H)

The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*].

| **SI-7** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_7\_role}} | |
| Parameter SI-7: {{si\_7\_parameter}} | |
| {{si\_7\_status}} | |
| {{si\_7\_origination}} | |

| **SI-7 What is the solution and how is it implemented?** |
| --- |
| {{si\_7\_implementation}} |

SI-7 (1) Control Enhancement (M) (H)

The information system performs an integrity check of [*Assignment: organization-defined software, firmware, and information*] [*FedRAMP Selection (one or more): at startup; at [FedRAMP Assignment: to include security-relevant events*]; [*FedRAMP Assignment: at least monthly*]].

| **SI-7 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_7\_1\_role}} | |
| Parameter SI-7(1)-1: {{si\_7\_1\_1\_parameter}} | |
| Parameter SI-7(1)-2: {{si\_7\_1\_2\_parameter}} | |
| Parameter SI-7(1)-3: {{si\_7\_1\_3\_parameter}} | |
| {{si\_7\_1\_status}} | |
| {{si\_7\_1\_origination}} | |

| **SI-7 (1) What is the solution and how is it implemented?** |
| --- |
| {{si\_7\_1\_implementation}} |

SI-7 (2) Control Enhancement (H)

The organization employs automated tools that provide notification to [*Assignment: organization- defined personnel or roles]*] upon discovering discrepancies during integrity verification.

| **SI-7 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_7\_2\_role}} | |
| Parameter SI-7 (2): {{si\_7\_2\_parameter}} | |
| {{si\_7\_2\_status}} | |
| {{si\_7\_2\_origination}} | |

| **SI-7 (2) What is the solution and how is it implemented?** |
| --- |
| {{si\_7\_2\_implementation}} |

SI-7 (5) Control Enhancement (H)

The information system automatically [*Selection (one or more): shuts the information system down; restarts the information system; implements* [*Assignment: organization-defined security safeguard*]] when integrity violations are discovered.

| **SI-7 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_7\_5\_role}} | |
| Parameter SI-7 (5): {{si\_7\_5\_parameter}} | |
| {{si\_7\_5\_status}} | |
| {{si\_7\_5\_origination}} | |

| **SI-7 (5) What is the solution and how is it implemented?** |
| --- |
| {{si\_7\_5\_implementation}} |

SI-7 (7) Control Enhancement (M) (H)

The organization incorporates the detection of unauthorized [*Assignment: organization-defined security-relevant changes to the information system*] into the organizational incident response capability.

| **SI-7 (7)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_7\_7\_role}} | |
| Parameter SI-07(7): {{si\_7\_7\_parameter}} | |
| {{si\_7\_7\_status}} | |
| {{si\_7\_7\_origination}} | |

| **SI-7 (7) What is the solution and how is it implemented?** |
| --- |
| {{si\_7\_7\_implementation}} |

SI-7 (14) Control Enhancement (H)

The organization:

1. Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and
2. Provides exceptions to the source code requirement only for compelling mission/ operational requirements and with the approval of the authorizing official.

| **SI-7 (14)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_7\_14\_role}} | |
| {{si\_7\_14\_status}} | |
| {{si\_7\_14\_origination}} | |

| **SI-7 (14) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{si\_7\_14\_a\_implementation}} |
| **Part b** | {{si\_7\_14\_b\_implementation}} |

SI-8 Spam Protection (M) (H)

The organization:

1. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
2. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policies and procedures.

| **SI-8** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_8\_role}} | |
| {{si\_8\_status}} | |
| {{si\_8\_origination}} | |

| **SI-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{si\_8\_a\_implementation}} |
| **Part b** | {{si\_8\_b\_implementation}} |

SI-8 (1) Control Enhancement (M) (H)

The organization centrally manages spam protection mechanisms.

| **SI-8 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_8\_1\_role}} | |
| {{si\_8\_1\_status}} | |
| {{si\_8\_1\_origination}} | |

| **SI-8 (1) What is the solution and how is it implemented?** |
| --- |
| {{si\_8\_1\_implementation}} |

SI-8 (2) Control Enhancement (M) (H)

The organization automatically updates spam protection mechanisms.

| **SI-8 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_8\_2\_role}} | |
| {{si\_8\_2\_status}} | |
| {{si\_8\_2\_origination}} | |

| **SI-8 (2) What is the solution and how is it implemented?** |
| --- |
| {{si\_8\_2\_implementation}} |

SI-10 Information Input Validation (M) (H)

The information system checks the validity of [*Assignment: organization-defined information inputs*].

| **SI-10** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_10\_role}} | |
| Parameter SI-10: {{si\_10\_parameter}} | |
| {{si\_10\_status}} | |
| {{si\_10\_origination}} | |

| **SI-10 What is the solution and how is it implemented?** |
| --- |
| {{si\_10\_implementation}} |

SI-11 Error Handling (M) (H)

The information system:

1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
2. Reveals error messages only to [*Assignment: organization-defined personnel or roles*].

| **SI-11** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_11\_role}} | |
| Parameter SI-11(b): {{si\_11\_b\_parameter}} | |
| {{si\_11\_status}} | |
| {{si\_11\_origination}} | |

| **SI-11 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | {{si\_11\_a\_implementation}} |
| **Part b** | {{si\_11\_b\_implementation}} |

SI-12 Information Output Handling and Retention (L) (M) (H)

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

| **SI-12** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_12\_role}} | |
| {{si\_12\_status}} | |
| {{si\_12\_origination}} | |

| **SI-12 What is the solution and how is it implemented?** | |
| --- | --- |
| **SI-12** | {{si\_12\_implementation}} |

SI-16 Memory Protection (M) (H)

The information system implements [*Assignment: organization-defined fail-safe procedures*] to protect its memory from unauthorized code execution.

| **SI-16** | **Control Summary Information** |
| --- | --- |
| Responsible Role: {{si\_16\_role}} | |
| Parameter SI-16-1: {{si\_16\_1\_parameter}} | |
| {{si\_16\_status}} | |
| {{si\_16\_origination}} | |

| **SI-16 What is the solution and how is it implemented?** |
| --- |
| {{si\_16\_implementation}} |

# Acronyms

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website [Documents](https://www.fedramp.gov/documents) page.

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.

Systems Security Plan Attachments

# Attachments

Table 15‑1. Names of Provided Attachments

|  |  |  |
| --- | --- | --- |
| Attachment | File Name | File Extension |
| * Information Security Policies and Procedures | O365 Information Security Policy 2020 | .docx |
| * User Guide | O365 User Guide | .docx |
| * Digital Identity Worksheet | Included in Section 15 |  |
| PTA | Included in Section 15 |  |
| PIA (if needed) | Office 365 MT PIA v5.1 | .docx |
| * Rules of Behavior | O365 MT Rules of Behavior v1.6 10.17.2019 | .docx |
| * Information System Contingency Plan | Multiple attachments, provided separately | .docx |
| * Configuration Management Plan | O365 Configuration Management Plan v1.7 03.22.19 | .docx |
| * Incident Response Plan | Incident Response Plan\_02.13.20 | .docx |
| * CIS Workbook | MT-GCC CIS Workbook v8.01 | .xlsx |
| * FIPS 199 | Included in Section 15 |  |
| * Inventory | GCC-MT\_Inventory | .xlsx |
| * Ports & Protocols | MT Dataflows | .xlsx |

## ATTACHMENT 1 - Information Security Policies and Procedures

All Authorization Packages must include an Information Security Policies and Procedures attachment, which will be reviewed for quality.

## ATTACHMENT 2 - User Guide

All Authorization Packages must include an Information Security Policies and Procedures attachment, which will be reviewed for quality.

## ATTACHMENT 3 - Digital Identity Worksheet

The Digital Identity section explains the objective for selecting the appropriate Digital Identity levels for the candidate system. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63, Revision 3, Digital Identity Guidelines.

### Introduction and Purpose

This document provides guidance on digital identity services (Digital Identity, which is the process of establishing confidence in user identities electronically presented to an information system). Authentication focuses on the identity proofing process (IAL), the authentication process (AAL), and the assertion protocol used in a federated environment to communicate authentication and attribute information (if applicable) (FAL). NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

NIST SP 800-63-3 can be found at the following URL: [NIST SP 800-63-3](https://pages.nist.gov/800-63-3/)

### Information System Name/Title

This Digital Identity Plan provides an overview of the security requirements for Office 365 in accordance with NIST SP 800-63-3.

Table 15‑2. Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| F1209231600 | Office 365 MultiTenant | Office 365 MT |

### Digital Identity Level Definitions

NIST SP 800-63-3 defines three levels in each of the components of identity assurance to categorize a federal information system’s Digital Identity posture. NIST SP 800-63-3 defines the Digital Identity levels as:

* IAL – refers to the identity proofing process.
* AAL – refers to the authentication process.
* FAL – refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).

FedRAMP maps its system categorization levels to NIST 800-63-3’s levels as shown in Table 15-3:

Table 15‑3. Mapping FedRAMP Levels to NIST SP 800-63-3 Levels

| FedRAMP System Categorization | Identity Assurance Level (IAL) | Authenticator Assurance Level (AAL) | Federation Assurance Level (FAL) |
| --- | --- | --- | --- |
| **High** | IAL3: In-person, or supervised remote identity proofing | AAL3: Multi-factor required based on hardware-based cryptographic authenticator and approved cryptographic techniques | FAL3: The subscriber (user) must provide proof of possession of a cryptographic key, which is referenced by the assertion. The assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it |
| **Moderate** | IAL2: In-person or remote, potentially involving a “trusted referee” | AAL2: Multi-factor required, using approved cryptographic techniques | FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it |
| **Low** | IAL1: Self-asserted | AAL1: Single-factor or multi-factor | FAL1: Assertion is digitally signed by the identity provider |
| **FedRAMP Tailored LI-SaaS** | IAL1: Self-asserted | AAL1: Single-factor or multi-factor | FAL1: Assertion is digitally signed by the identity provider |

Selecting the appropriate Digital Identity level for a system enables the system owner to determine the right system authentication technology solution for the selected Digital Identity levels. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63-3.

### Review Maximum Potential Impact Levels

Microsoft has assessed the potential risk from Digital Identity errors, or Digital Identity misuse, related to a user’s asserted identity. Microsoft has taken into consideration the potential for harm (impact) and the likelihood of the occurrence of the harm and has identified an impact profile as found in Table 15‑4 Potential Impacts for Assurance Levels.

Assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Table 15‑4. Potential Impacts for Assurance Levels

|  | Assurance Level Impact Profile | | |
| --- | --- | --- | --- |
| Potential Impact Categories | 1 | 2 | 3 |
| Inconvenience, distress or damage to standing or reputation | Low | Mod | High |
| Financial loss or agency liability | Low | Mod | High |
| Harm to agency programs or public interests | N/A | Low/Mod | High |
| Unauthorized release of sensitive information | N/A | Low/Mod | High |
| Personal Safety | N/A | Low | Mod/High |
| Civil or criminal violations | N/A | Low/Mod | High |

### Digital Identity Level Selection

The Microsoft has identified that they support the Digital Identity Level that has been selected for the Office 365 MT as noted in Table 15‑5 Digital Identity Level. The selected Digital Identity Level indicated is supported for federal agency consumers of the cloud service offering. Implementation details of the Digital Identity mechanisms are provided in the System Security Plan under control IA-2.

Table 15‑5. Digital Identity Level

| Digital Identity Level | Maximum Impact Profile | Selection |
| --- | --- | --- |
| Level 1: AAL1, IAL1, FAL1 | Low | ☐ |
| Level 2: AAL2, IAL2, FAL2 | Moderate | ☐ |
| Level 3: AAL3, IAL3, FAL3 | High | ☒ |

## ATTACHMENT 4 - PTA / PIA

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/templates).

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in ATTACHMENT 12 – FedRAMP Laws and Regulations.

### Privacy Overview and Point of Contact (POC)

The Table 15‑6. Office 365 MT Privacy POC individual is identified as the Office 365 MT; Privacy Officer and POC for privacy at Microsoft.

Table 15‑6. Office 365 MT Privacy POC

| Name | Greg Roberts |
| --- | --- |
| Title | Microsoft Office 365 Principal Group Program Manager |
| CSP / Organization | Microsoft / O365 |
| Address | 1 Microsoft Way, Redmond, WA 98052 |
| Phone Number | +1 (425) 722-6538 |
| Email Address | groberts@microsoft.com |

#### Applicable Laws and Regulations

The FedRAMP Laws and Regulations may be found on: [Templates](https://www.fedramp.gov/templates). A summary of FedRAMP Laws and Regulations is included in the System Security Plan (SSP) ATTACHMENT 12 – FedRAMP Laws and Regulations.

Table 12-1 Office 365 Law and Regulations includes additional laws and regulations specific to Office 365.

Table 12‑1. Office 365 Laws and Regulations include additional laws and regulations that are specific to Office 365 MT. These will include laws and regulations from the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), United States Code (USC), and Homeland Security Presidential Directives (HSPD).

Table 15‑7. Office 365 MT Laws and Regulations

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
|  |  |  |  |

#### Applicable Standards and Guidance

The FedRAMP Standards and Guidance may be found on: [Templates](https://www.fedramp.gov/templates). The FedRAMP Standards and Guidance is included in the System Security Plan (SSP) ATTACHMENT 12 – FedRAMP Laws and Regulations. For more information, see the FedRAMP website.

Table 12‑2. Office 365 MT Standards and Guidance includes any additional standards and guidance that are specific to Office 365 MT. These will include standards and guidance from Federal Information Processing Standard (FIPS) and National Institute of Standards and Technology (NIST) Special Publications (SP).

Table 15‑8. Office 365 MT Standards and Guidance

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
|  | Department of Defense Cloud Computing Security Requirements Guide V1 R3 | 12/18/17 | [DISA SRG 1.3](https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf) |

#### Personally Identifiable Information (PII)

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

* + Social Security numbers
  + Passport numbers
  + Driver’s license numbers
  + Biometric information
  + DNA information
  + Bank account numbers

PII does not refer to business information or government information that cannot be traced back to an individual person.

### Privacy Threshold Analysis

Microsoft performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the Office 365 MT components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by Microsoft can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

#### Qualifying Questions

|  |  |
| --- | --- |
| Yes | 1. Does the ISA collect, maintain, or share PII in any identifiable form? |
| No | 1. Does the ISA collect, maintain, or share PII information from or about the public? |
| Yes | 1. Has a Privacy Impact Assessment ever been performed for the ISA? |
| No | 1. Is there a Privacy Act System of Records Notice (SORN) for this ISA system?  If yes; the SORN identifier and name is: |

If answers to Questions 1-4 are all “No” then a Privacy Impact Assessment may be omitted. If any of the answers to Question 1-4 are “Yes” then complete a Privacy Impact Assessment.

#### Designation

Check one.

|  |  |
| --- | --- |
| ☒ | A Privacy Sensitive System |
| ☐ | Not a Privacy Sensitive System (in its current version) |

The Privacy Impact Assessment Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/templates).

## ATTACHMENT 5 - Rules of Behavior

All Authorization Packages must include a Rules of Behavior (RoB) attachment, which will be reviewed for quality.

The RoB describes controls associated with user responsibilities and certain expectations of behavior for following security policies, standards and procedures. Security control PL-4 requires a CSP to implement rules of behavior.

The Rules of Behavior Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/templates).

The Template provides two example sets of rules of behavior: one for Internal Users and one for External Users. The CSP should modify each of these two sets to define the rules of behavior necessary to secure their system.

## ATTACHMENT 6 - Information System Contingency Plan

All Authorization Packages must include an Information System Contingency Plan attachment, which will be reviewed for quality.

The Information System Contingency Plan Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/templates).

The Information System Contingency Plan Template is provided for CSPs, 3PAOs, government contractors working on FedRAMP projects, government employees working on FedRAMP projects and any outside organizations that want to make use of the FedRAMP Contingency Planning process.

## ATTACHMENT 7 - Configuration Management Plan

All Authorization Packages must include a Configuration Management Plan attachment, which will be reviewed for quality.

## ATTACHMENT 8 - Incident Response Plan

All Authorization Packages must include an Incident Response Plan attachment, which will be reviewed for quality.

## ATTACHMENT 9 - CIS Workbook

All Authorization Packages must include Control Implementation Summary (CIS) Workbook attachment, which will be reviewed for quality.

The Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/templates).

## ATTACHMENT 10 - FIPS 199

All Authorization Packages must include a Federal Information Processing Standard (FIPS) 199 Section, which will be reviewed for quality.

The FIPS-199 Categorization report includes the determination of the security impact level for the cloud environment that may host any or all of the service models: IaaS, PaaS and SaaS. The ultimate goal of the security categorization is for the CSP to be able to select and implement the FedRAMP security controls applicable to its environment.

### Introduction and Purpose

This section is intended to be used by service providers who are applying for an Authorization through the U.S. federal government FedRAMP program.

The Federal Information Processing Standard 199 (FIPS 199) Categorization (Security Categorization) report is a key document in the security authorization package developed for submission to the Federal Risk and Authorization Management Program (FedRAMP) authorizing officials. The FIPS199 Categorization report includes the determination of the security impact level for the cloud environment that may host any or all of the service models (Information as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The ultimate goal of the security categorization is for the cloud service provider (CSP) to be able to select and implement the FedRAMP security controls applicable to its environment.

The purpose of the FIPS199 Categorization report is for the CSP to assess and complete the categorization of their cloud environment, to provide the categorization to the System Owner/Certifier and the FedRAMP Joint Authorization Board (JAB) and in helping them to make a determination of the CSP’s ability to host systems at that level. The completed security categorization report will aid the CSP in selection and implementation of FedRAMP security controls at the determined categorization level.

### Scope

The scope of the FIPS199 Categorization report includes the assessment of the information type categories as defined in the NIST Special Publication 800-60 Volume II Revision 1 Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.

### System Description

Office 365 MT has been determined to have a security categorization of High (H).

### Methodology

Impact levels are determined for each information type based on the security objectives (confidentiality, integrity, availability). The confidentiality, integrity, and availability impact levels define the security sensitivity category of each information type. The FIPS PUB 199 is the high watermark for the impact level of all the applicable information types.

The FIPS PUB 199 analysis represents the information type and sensitivity levels of the CSP’s cloud service offering (and is not intended to include sensitivity levels of agency data). Customer agencies will be expected to perform a separate FIPS 199 Categorization report analysis for their own data hosted on the CSP’s cloud environment. The analysis must be added as an appendix to the SSP and drive the results for the Categorization section

The Table 15‑9 CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1below uses the NIST SP 800-60 V2 R1 Volume II Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories to identify information types with the security impacts.

Table 15‑9. CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1

| Information Type | NIST SP 800-60 V2 R1  Recommended Confidentiality Impact Level | NIST SP 800-60 V2 R1  Recommended Integrity Impact Level | NIST SP 800-60 V2 R1  Recommended Availability Impact Level | CSP Selected Confidentiality Impact Level | CSP Selected Integrity Impact Level | CSP Selected Availability Impact Level | Statement  for Impact Adjustment Justification |
| --- | --- | --- | --- | --- | --- | --- | --- |
| System Development | Low | Moderate | Low | Low | Moderate | Low |  |
| Lifecycle/Change Management | Low | Moderate | Low | Low | Moderate | Low |  |
| System Maintenance | Low | Moderate | Low | Low | Moderate | Low |  |
| IT Infrastructure Maintenance | Low | Low | Low | Low | Low | Low |  |
| Information Security | Low | Moderate | Moderate | Low | Moderate | Moderate |  |
| Record Retention | Low | Low | Low | Low | Low | Low |  |
| Information Management | Low | Moderate | Low | Low | Moderate | Low |  |
| System and Network Monitoring | Moderate | Moderate | Low | Moderate | Moderate | Low |  |
| Information Sharing | Low | Low | Moderate | Low | Low | Moderate |  |
| System Development | Low | Moderate | Low | Low | Moderate | Low |  |
| Lifecycle/Change Management | Low | Moderate | Low | Low | Moderate | Low |  |
| System Maintenance | Low | Moderate | Low | Low | Moderate | Low |  |
| IT Infrastructure Maintenance | Low | Low | Low | Low | Low | Low |  |

## ATTACHMENT 11 - Separation of Duties Matrix

All Authorization Packages have the option to provide a Separation of Duties Matrix attachment, which will be reviewed for quality.

As stated in AC-05(b): The separation of duties is documented through eligibilities (roles) assigned to service team administrators in account management tools.

## ATTACHMENT 12 - FedRAMP Laws and Regulations

The Table 15‑8 FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance lists all of the FedRAMP templates in which FedRAMP laws, regulations, standards and guidance are referenced.

Table 15‑10. FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance

| Phase | Document Title | |
| --- | --- | --- |
| Document Phase | SSP | System Security Plan |
| SSP Attachment 4 | PTA/PIA | Privacy Threshold Analysis and Privacy Impact Assessment |
| SSP Attachment 6 | ISCP | Information System Contingency Plan |
| SSP Attachment 10 | FIPS 199 | FIPS 199 Categorization |
| Assess Phase | SAP | Security Assessment Plan |
| Authorize Phase | SAR | Security Assessment Report |

The FedRAMP Laws and Regulations can be submitted as an appendix or an attachment. The attachment can be found on this page: [Templates](https://www.fedramp.gov/templates).

Note: All NIST Computer Security Publications can be found at the following  
URL: <http://csrc.nist.gov/publications/PubsSPs.html>

## ATTACHMENT 13 - FedRAMP Inventory Workbook

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

* System Security Plan
* Security Assessment Plan
* Security Assessment Report
* Information System Contingency Plan
* Initial POAM
* Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/templates).

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

## ATTACHMENT 14 – Ports, Protocols, and Services

The Ports, Protocols, & Services in use in Office 365 will be provided as an attachment. This attachment has been provided separately to the 3PAO.

## ATTACHMENT 15 – Office 365 Internal Documents

This section is to list the Office 365 internal documents noted in this SSP that are onsite for auditor review. It is not a separate attachment.

Table 15-10 Office 365 Internal Documents

|  |
| --- |
| Document Name |
| Microsoft Documentation Retention Policy |
| Microsoft Enterprise Online Services Data Taxonomy (aka Asset Classification Standard) |
| Office 365 Data Handling Standard |
| Active Framework Controls |
| Office 365 Risk Management SOP |
| Office 365 with Support Standard Operating Procedures (SOPs)  (formerly Office ITAR Defense) |
| Office 365 Continuous Monitoring Strategy Guide |