| **FedRAMP System Security Plan (SSP) Moderate Baseline Template**  Cloud Service Provider Name  Information System Name  Version #  Version Date |
| --- |

****

*Instruction: This template contains a number of features to facilitate data entry. As you go through the template entering data, you will see prompts for you to enter different types of data.*

*Repeatable Field*

*Some multiple-occurring data fields have been linked together and you need only enter the data once. Enter the data once; then click outside the data entry field and all occurrences of that field will be populated. For example, when you see “Information System Abbreviation” and replace it with your system abbreviation, all instances of the abbreviation throughout the document will be replaced with the value you entered. This document contains the following repeatable fields:*

*CSP Name*

*Information System Name*

*Version Number*

*Version Date*

*Information System Abbreviation*

*If you find a data field from the above list that has not populated, then press the F9 key to refresh the data. If you make a change to one of the above data fields, you may also have to press the F9 key to refresh the data throughout the document. Remember to save the document after refreshes. The one exception to the repeatable fields is information system names for FedRAMP or leveraged authorizations that are identified as “Leveraged information system name:*

*Date Selection*

*Data fields that must contain a date will present a date selection menu.*

*Item Choice*

*Data fields that have a limited number of value choices will present a selection list.*

*Number Entry*

*Data fields that must have numeric values display “number.”*

*Text Entry*

*Many data fields, particularly in tables, that can contain any text display “Enter text” or “Click here to enter text.”*

*Delete this instruction from your final version of this document.*

**System Security Plan**

**Prepared by**

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

**Prepared for**

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

**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 | Reformatted to FedRAMP Document Standard, added repeated text schema and content fields to tables that were not Control Tables.  Revised cover page, changed document designation to Controlled Unclassified Information (CUI),  Removed front matter section How This Document is Organized, Instructions re-written,  Corrected section numbering to match SSP v1.0,  Revised Section 9 Table 9-1 Personnel Roles and Privileges, Removed Section 10 inventory tables (see Attachment 13 FedRAMP Inventory Workbook).  Global verbiage change, Authorizing Official (AO) changed to JAB/AO; e-Authentication, e-authentication and E-authentication changed to E-Authentication.  Added attachments 10 FIPS 199, 11 Separation of Duties Matrix, 12 FedRAMP Laws and Regulations, 13 FedRAMP Inventory Workbook.  Changes to the following controls: AC-02 (05), AC-05, AC-17 (09), AU-03 (01), AU-05, AU-06, CA-02 (03), CA-7, CM-02 (01), IA-02 (11), MP-03, PL-08, SA-09 (01), SC-15, SI-04 (04) |
| 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 Sec 10 and Attachment 13  Removed chapter numbers from Attachments  Removed 3 questions from Sec 2.3 E-Authentication Determination |
| 3/6/2017 | Document renamed from "FedRAMP System Security Plan (SSP) Moderate Baseline Master Template to "FedRAMP System Security Plan (SSP) Moderate Baseline Template” |
| 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 |
| 5/18/2021 | Revised SA-4 Additional FedRAMP Requirements and Guidance |

**Document Revision History**

| Date | Description | Version of SSP | Author |
| --- | --- | --- | --- |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

**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)

*Instruction: The System Security Plan is the main document in which the Cloud Service Provider (CSP) describes all the security controls in use on the information system and their implementation.*

*This document is released in template format. Once populated with content, this document will include detailed information about service provider information security controls.*

*This document is intended to be used by service providers who are applying for a Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO) or an Agency Authorization to Operate (ATO) through the Federal Risk and Authorization Management Program (FedRAMP).   
  
In the sections that follow, describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage and monitor the control. In some cases, the responsibility is shared by a CSP and by the customer. Use the definitions in the table that follows to indicate where each security control originates from.*

Note that “-1” Controls (AC-1, AU-1, SC-1, etc.)\* cannot be inherited and must be described in some way by the service provider.  
\*Access Control (AC), Audit and Accountability (AU), System and Communications Protection (SC)

*Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.*

*For System as a Service (SaaS) and Platform as a Service (PaaS) systems that are inheriting controls from an Infrastructure as a Service (IaaS) (or anything lower in the stack), the “inherited” check box must be checked and the implementation description must simply say “inherited.” FedRAMP reviewers will determine whether the control-set is appropriate or not.*

*In Section 13, the National Institute of Standards and Technology (NIST) term "organization defined" must be interpreted as being the CSP's responsibility unless otherwise indicated. In some cases the JAB has chosen to define or provide parameters, in others they have left the decision up to the CSP.*

*Delete this instruction from your final version of this document.*

**TABLE OF CONTENTS**

[**1.**](#_2et92p0) **Information System Name/Title 1**

[**2.**](#_3dy6vkm) **Information System Categorization 1**

[**2.1.**](#_4d34og8) **Information Types 1**

[**2.2.**](#_17dp8vu) **Security Objectives Categorization (FIPS 199) 3**

[**2.3.**](#_lnxbz9) **Digital Identity Determination 4**

[**3.**](#_35nkun2) **Information System Owner 4**

[**4.**](#_44sinio) **Authorizing Official 4**

[**5.**](#_2jxsxqh) **Other Designated Contacts 5**

[**6.**](#_4i7ojhp) **Assignment of Security Responsibility 6**

[**7.**](#_3whwml4) **Information System Operational Status 7**

[**8.**](#_qsh70q) **Information System Type 7**

[**8.1.**](#_3as4poj) **Cloud Service Models 7**

[**8.2.**](#_2p2csry) **Cloud Deployment Models 8**

[**8.3.**](#_3o7alnk) **Leveraged Authorizations 9**

[**9.**](#_ihv636) **General System Description 9**

[**9.1.**](#_32hioqz) **System Function or Purpose 9**

[**9.2.**](#_41mghml) **Information System Components and Boundaries 10**

[**9.3.**](#_vx1227) **Types of Users 11**

[**9.4.**](#_1v1yuxt) **Network Architecture 12**

[**10.**](#_2u6wntf) **System Environment And Inventory 12**

[**10.1.**](#_19c6y18) **Data Flow 14**

[**10.2.**](#_28h4qwu) **Ports, Protocols and Services 14**

[**11.**](#_37m2jsg) **System Interconnections 16**

[**12.**](#_2lwamvv) **Laws, Regulations, Standards and Guidance 18**

[**12.1.**](#_111kx3o) **Applicable Laws and Regulations 18**

[**12.2.**](#_206ipza) **Applicable Standards and Guidance 18**

[**13.**](#_2zbgiuw) **Minimum Security Controls 19**

[**13.1.**](#_2dlolyb) **Access Control (AC) 26**

[AC-1 Access Control Policy and Procedures Requirements (L) (M) 26](#_sqyw64)

[AC-2 Account Management (L) (M) 27](#_1rvwp1q)

[AC-2 (1) Control Enhancement (M) (H) 29](#_kgcv8k)

[AC-2 (2) Control Enhancement (M) 30](#_34g0dwd)

[AC-2 (3) Control Enhancement (M) 30](#_1jlao46)

[AC-2 (4) Control Enhancement (M) 31](#_43ky6rz)

[AC-2 (5) Control Enhancement (M) 32](#_2iq8gzs)

[AC-2 (7) Control Enhancement (M) 33](#_xvir7l)

[AC-2 (9) Control Enhancement (M) 33](#_3hv69ve)

[AC-2 (10) Control Enhancement (M) (H) 34](#_1x0gk37)

[AC-2 (12) Control Enhancement (M) 35](#_4h042r0)

[AC-3 Access Enforcement (L) (M) (H) 36](#_2w5ecyt)

[AC-4 Information Flow Enforcement (M) (H) 36](#_1baon6m)

[AC-4 (21) Control Enhancement (M) (H) 37](#_3vac5uf)

[AC-5 Separation of Duties (M) (H) 38](#_2afmg28)

[AC-6 Least Privilege (M) (H) 39](#_pkwqa1)

[AC-6 (1) Control Enhancement (M) 39](#_39kk8xu)

[AC-6 (2) Control Enhancement (M) (H) 40](#_1opuj5n)

[AC 6 (5) Control Enhancement (M) (H) 41](#_48pi1tg)

[AC-6 (9) Control Enhancement (M) (H) 42](#_2nusc19)

[AC-6 (10) Control Enhancement (M) (H) 42](#_1302m92)

[AC-7 Unsuccessful Login Attempts (L) (M) 43](#_3mzq4wv)

[AC-8 System Use Notification (L) (M) (H) 44](#_319y80a)

[AC-10 Concurrent Session Control (M) (H) 46](#_1gf8i83)

[AC-11 Session Lock (M) (H) 47](#_2fk6b3p)

[AC-11 (1) Control Enhancement (M) (H) 48](#_upglbi)

[AC-12 Session Termination (M) (H) 49](#_3ep43zb)

[AC-14 Permitted Actions without Identification or Authentication (L) (M) (H) 49](#_1tuee74)

[AC-17 Remote Access (L) (M) (H) 50](#_2szc72q)

[AC-17 (1) Control Enhancement (M) (H) 51](#_184mhaj)

[AC-17 (2) Control Enhancement (M) (H) 52](#_3s49zyc)

[AC-17 (3) Control Enhancement (M) (H) 52](#_279ka65)

[AC-17 (4) Control Enhancement (M) (H) 53](#_36ei31r)

[AC-17 (9) Control Enhancement (M) (H) 54](#_45jfvxd)

[AC-18 Wireless Access Restrictions (L) (M) (H) 54](#_2koq656)

[AC-18 (1) Control Enhancement (M) (H) 55](#_zu0gcz)

[AC-19 Access Control for Portable and Mobile Systems (L) (M) (H) 56](#_3jtnz0s)

[AC-19 (5) Control Enhancement (M) (H) 57](#_1yyy98l)

[AC-20 Use of External Information Systems (L) (M) (H) 57](#_4iylrwe)

[AC-20 (1) Control Enhancement (M) (H) 58](#_2y3w247)

[AC-20 (2) Control Enhancement (M) (H) 59](#_1d96cc0)

[AC-21 Information Sharing (M) (H) 60](#_3x8tuzt)

[AC-22 Publicly Accessible Content (L) (M) (H) 61](#_2ce457m)

[**13.2.**](#_rjefff) **Awareness and Training (AT) 62**

[AT-1 Security Awareness and Training Policy and Procedures (L) (M) 62](#_3bj1y38)

[AT-2 Security Awareness (L) (M) (H) 63](#_1qoc8b1)

[AT-2 (2) Control Enhancement (M) (H) 63](#_4anzqyu)

[AT-3 Role-Based Security Training (L) (M) (H) 64](#_2pta16n)

[AT-4 Security Training Records (L) (M) 65](#_14ykbeg)

[**13.3.**](#_3oy7u29) **Audit and Accountability (AU) 66**

[AU-1 Audit and Accountability Policy and Procedures (L) (M) 66](#_243i4a2)

[AU-2 Audit Events (L) (M) (H) 67](#_j8sehv)

[AU-2 (3) Control Enhancement (M) (H) 68](#_338fx5o)

[AU-3 Content of Audit Records (L) (M) (H) 69](#_1idq7dh)

[AU-3 (1) Control Enhancement (M) 69](#_42ddq1a)

[AU-4 Audit Storage Capacity (L) (M) (H) 70](#_2hio093)

[AU-5 Response to Audit Processing Failures (L) (M) (H) 71](#_wnyagw)

[AU-6 Audit Review, Analysis, and Reporting (L) (M) (H) 72](#_3gnlt4p)

[AU-6 (1) Control Enhancement (M) (H) 73](#_4fsjm0b)

[AU-6 (3) Control Enhancement (M) (H) 73](#_2uxtw84)

[AU-7 Audit Reduction and Report Generation (M) (H) 74](#_1a346fx)

[AU-7 (1) Control Enhancement (M) (H) 75](#_3u2rp3q)

[AU-8 Time Stamps (L) (M) (H) 76](#_2981zbj)

[AU-8 (1) Control Enhancement (M) (H) 76](#_odc9jc)

[AU-9 Protection of Audit Information (L) (M) (H) 78](#_38czs75)

[AU-9 (2) Control Enhancement (M) (H) 78](#_1nia2ey)

[AU-9 (4) Control Enhancement (M) (H) 79](#_47hxl2r)

[AU-11 Audit Record Retention (M) 80](#_2mn7vak)

[AU-12 Audit Generation (L) (M) (H) 80](#_11si5id)

[**13.4.**](#_20xfydz) **Security Assessment and Authorization (CA) 81**

[CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M) 81](#_4kx3h1s)

[CA-2 Security Assessments (L) (M) (H) 82](#_302dr9l)

[CA-2 (1) Control Enhancement (L) (M) (H) 84](#_1f7o1he)

[CA-2 (2) Control Enhancement (M) (H) 84](#_3z7bk57)

[CA-2 (3) Control Enhancement (M) (H) 85](#_2eclud0)

[CA-3 System Interconnections (L) (M) (H) 86](#_3dhjn8m)

[CA-3 (3) Control Enhancement (M) (H) 88](#_16x20ju)

[CA-3 (5) Control Enhancement (M) 88](#_3qwpj7n)

[CA-5 Plan of Action and Milestones (L) (M) (H) 89](#_261ztfg)

[CA-6 Security Authorization (L) (M) (H) 90](#_l7a3n9)

[CA-7 Continuous Monitoring (L) (M) (H) 91](#_356xmb2)

[CA-7 (1) Control Enhancement (M) (H) 94](#_1kc7wiv)

[CA-8 Penetration Testing (M) (H) 94](#_44bvf6o)

[CA-8 (1) Control Enhancement (M) (H) 95](#_2jh5peh)

[CA-9 Internal System Connections (L) (M) (H) 96](#_ymfzma)

[**13.5.**](#_3im3ia3) **Configuration Management (CM) 97**

[CM-1 Configuration Management Policies and Procedures (L) (M) 97](#_1xrdshw)

[CM-2 Baseline Configuration (L) (M) (H) 98](#_4hr1b5p)

[CM-2 (1) Control Enhancement (M) 98](#_2wwbldi)

[CM-2 (2) Control Enhancement (M) (H) 99](#_1c1lvlb)

[CM-2 (3) Control Enhancement (M) 100](#_3w19e94)

[CM-2 (7) Control Enhancement (M) (H) 100](#_2b6jogx)

[CM-3 Configuration Change Control (M) (H) 101](#_qbtyoq)

[CM-4 Security Impact Analysis (L) (M) (H) 103](#_3abhhcj)

[CM-5 Access Restrictions for Change (M) (H) 103](#_1pgrrkc)

[CM-5 (1) Control Enhancement (M) (H) 104](#_49gfa85)

[CM-5 (3) Control Enhancement (M) (H) 105](#_2olpkfy)

[CM-5 (5) Control Enhancement (M) (H) 105](#_13qzunr)

[CM-6 Configuration Settings (L) (M) (H) 106](#_3nqndbk)

[CM-6 (1) Control Enhancement (M) (H) 108](#_22vxnjd)

[CM-7 Least Functionality (L) (M) (H) 108](#_i17xr6)

[CM-7 (1) Control Enhancement (M) (H) 109](#_1h65qms)

[CM-7 (2) Control Enhancement (M) (H) 110](#_415t9al)

[CM-7 (5) Control Enhancement (M) 111](#_vgdtq7)

[CM-8 Information System Component Inventory (L) (M) (H) 112](#_3fg1ce0)

[CM-8 (1) Control Enhancement (M) (H) 113](#_1ulbmlt)

[CM-8 (3) Control Enhancement (M) (H) 114](#_4ekz59m)

[CM-8 (5) Control Enhancement (M) (H) 115](#_2tq9fhf)

[CM-9 Configuration Management Plan (M) (H) 115](#_18vjpp8)

[CM-10 Software Usage Restrictions (L) (M) (H) 116](#_3sv78d1)

[CM-10 (1) Control Enhancement (M) (H) 117](#_n5rssn)

[CM-11 User-Installed Software (M) (H) 118](#_375fbgg)

[**13.6.**](#_1maplo9) **Contingency Planning (CP) 119**

[CP-1 Contingency Planning Policy and Procedures (L) (M) 119](#_46ad4c2)

[CP-2 Contingency Plan (L) (M) (H) 120](#_2lfnejv)

[CP-2 (1) Control Enhancement (M) (H) 121](#_10kxoro)

[CP-2 (2) Control Enhancement (M) (H) 122](#_3kkl7fh)

[CP-2 (3) Control Enhancement (M) (H) 123](#_1zpvhna)

[CP-2 (8) Control Enhancement (M) (H) 123](#_4jpj0b3)

[CP-3 Contingency Training (L) (M) (H) 124](#_2yutaiw)

[CP-4 Contingency Plan Testing (M) 125](#_1e03kqp)

[CP-4 (1) Control Enhancement (M) (H) 126](#_3xzr3ei)

[CP-6 Alternate Storage Site (M) (H) 127](#_2d51dmb)

[CP-6 (1) Control Enhancement (M) (H) 127](#_sabnu4)

[CP-6 (3) Control Enhancement (M) (H) 128](#_3c9z6hx)

[CP-7 Alternate Processing Site (M) (H) 129](#_1rf9gpq)

[CP-7 (1) Control Enhancement (M) (H) 130](#_4bewzdj)

[CP-7 (2) Control Enhancement (M) (H) 131](#_2qk79lc)

[CP-7 (3) Control Enhancement (M) (H) 131](#_15phjt5)

[CP-8 Telecommunications Services (M) (H) 132](#_3pp52gy)

[CP-8 (1) Control Enhancement (M) (H) 133](#_24ufcor)

[CP-8 (2) Control Enhancement (M) (H) 134](#_jzpmwk)

[CP-9 Information System Backup (L) (M) (H) 134](#_33zd5kd)

[CP-9 (1) Control Enhancement (M) 136](#_1j4nfs6)

[CP-9 (3) Control Enhancement (M) (H) 136](#_434ayfz)

[CP-10 Information System Recovery and Reconstitution (L) (M) (H) 137](#_2i9l8ns)

[CP-10 (2) Control Enhancement (M) (H) 138](#_xevivl)

[**13.7.**](#_3hej1je) **Identification and Authentication (IA) 138**

[IA-1 Identification and Authentication Policy and Procedures (L) (M) 138](#_1wjtbr7)

[IA-2 User Identification and Authentication (L) (M) (H) 139](#_4gjguf0)

[IA-2 (1) Control Enhancement (L) (M) (H) 140](#_2vor4mt)

[IA-2 (2) Control Enhancement (M) (H) 141](#_1au1eum)

[IA-2 (3) Control Enhancement (M) (H) 141](#_3utoxif)

[IA-2 (5) Control Enhancement (M) (H) 142](#_29yz7q8)

[IA-2 (8) Control Enhancement (M) (H) 143](#_p49hy1)

[IA-2 (11) Control Enhancement (M) (H) 143](#_393x0lu)

[IA-2 (12) Control Enhancement (L) (M) (H) 144](#_1o97atn)

[IA-3 Device Identification and Authentication (M) (H) 145](#_488uthg)

[IA-4 Identifier Management (L) (M) 146](#_2ne53p9)

[IA-4 (4) Control Enhancement (M) (H) 147](#_12jfdx2)

[IA-5 Authenticator Management (L) (M) 148](#_3mj2wkv)

[IA-5 (1) Control Enhancement (L) (M) 149](#_21od6so)

[IA-5 (2) Control Enhancement (M) (H) 150](#_gtnh0h)

[IA-5 (3) Control Enhancement (M) (H) 151](#_30tazoa)

[IA-5 (4) Control Enhancement (M) 152](#_1fyl9w3)

[IA-5 (6) Control Enhancement (M) (H) 153](#_3zy8sjw)

[IA-5 (7) Control Enhancement (M) (H) 154](#_2f3j2rp)

[IA-5 (11) Control Enhancement (L) (M) (H) 154](#_u8tczi)

[IA-6 Authenticator Feedback (L) (M) (H) 155](#_3e8gvnb)

[IA-7 Cryptographic Module Authentication (L) (M) (H) 156](#_1tdr5v4)

[IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H) 156](#_4ddeoix)

[IA-8 (1) Control Enhancement (L) (M) (H) 157](#_2sioyqq)

[IA-8 (2) Control Enhancement (L) (M) (H) 158](#_3rnmrmc)

[IA-8 (3) Control Enhancement (L) (M) (H) 158](#_26sx1u5)

[IA-8 (4) Control Enhancement (L) (M) (H) 159](#_ly7c1y)

[**13.8.**](#_35xuupr) **Incident Response (IR) 160**

[IR-1 Incident Response Policy and Procedures (L) (M) 160](#_1l354xk)

[IR-2 Incident Response Training (L) (M) 161](#_452snld)

[IR-3 Incident Response Testing (M) 161](#_2k82xt6)

[IR-3 (2) Control Enhancement (M) (H) 162](#_zdd80z)

[IR-4 Incident Handling (L) (M) (H) 163](#_3jd0qos)

[IR-4 (1) Control Enhancement (M) (H) 164](#_1yib0wl)

[IR-5 Incident Monitoring (L) (M) (H) 165](#_4ihyjke)

[IR-6 Incident Reporting (L) (M) (H) 165](#_2xn8ts7)

[IR-6 (1) Control Enhancement (M) (H) 166](#_1csj400)

[IR-7 Incident Response Assistance (L) (M) (H) 167](#_3ws6mnt)

[IR-7 (1) Control Enhancement (M) (H) 168](#_2bxgwvm)

[IR-7 (2) Control Enhancement (M) (H) 168](#_r2r73f)

[IR-8 Incident Response Plan (L) (M) (H) 169](#_3b2epr8)

[IR-9 Information Spillage Response (M) (H) 171](#_1q7ozz1)

[IR-9 (1) Control Enhancement (M) (H) 172](#_4a7cimu)

[IR-9 (2) Control Enhancement (M) 172](#_2pcmsun)

[IR-9 (3) Control Enhancement (M) (H) 173](#_14hx32g)

[IR-9 (4) Control Enhancement (M) (H) 174](#_3ohklq9)

[**13.9.**](#_23muvy2) **Maintenance (MA) 175**

[MA-1 System Maintenance Policy and Procedures (L) (M) 175](#_is565v)

[MA-2 Controlled Maintenance (L) (M) (H) 176](#_32rsoto)

[MA-3 Maintenance Tools (M) (H) 177](#_1hx2z1h)

[MA-3 (1) Control Enhancement (M) (H) 177](#_41wqhpa)

[MA-3 (2) Control Enhancement (M) (H) 178](#_2h20rx3)

[MA-3 (3) Control Enhancement (M) (H) 179](#_w7b24w)

[MA-4 Remote Maintenance (L) (M) (H) 180](#_3g6yksp)

[MA-4 (2) Control Enhancement (M) (H) 181](#_1vc8v0i)

[MA-5 Maintenance Personnel (L) (M) (H) 181](#_4fbwdob)

[MA-5 (1) Control Enhancement (L) (M) 182](#_2uh6nw4)

[MA-6 Timely Maintenance (M) (H) 183](#_19mgy3x)

[**13.10.**](#_3tm4grq) **Media Protection (MP) 184**

[MP-1 Media Protection Policy and Procedures (L) (M) 184](#_28reqzj)

[MP-2 Media Access (L) (M) 185](#_nwp17c)

[MP-3 Media Labeling (M) (H) 186](#_37wcjv5)

[MP-4 Media Storage (M) (H) 187](#_1n1mu2y)

[MP-5 Media Transport (M) (H) 188](#_471acqr)

[MP-5 (4) Control Enhancement (M) (H) 189](#_2m6kmyk)

[MP-6 Media Sanitization and Disposal (L) (M) 189](#_11bux6d)

[MP-6 (2) Control Enhancement (M) 190](#_3lbifu6)

[MP-7 Media Use (L) (M) (H) 191](#_20gsq1z)

[MP-7 (1) Control Enhancement (M) (H) 192](#_4kgg8ps)

[**13.11.**](#_2zlqixl) **Physical and Environmental Protection (PE) 192**

[PE-1 Physical and Environmental Protection Policy and Procedures (L) (M) 192](#_1er0t5e)

[PE-2 Physical Access Authorizations (L) (M) 193](#_3yqobt7)

[PE-3 Physical Access Control (L) (M) (H) 194](#_2dvym10)

[PE-4 Access Control for Transmission Medium (M) (H) 196](#_3d0wewm)

[PE-5 Access Control for Output Devices (M) (H) 197](#_1s66p4f)

[PE-6 Monitoring Physical Access (L) (M) (H) 197](#_4c5u7s8)

[PE-6 (1) Control Enhancement (M) (H) 198](#_2rb4i01)

[PE-8 Visitor Access Records (L) (M) (H) 199](#_16ges7u)

[PE-9 Power Equipment and Cabling (M) (H) 200](#_3qg2avn)

[PE-10 Emergency Shutoff (M) (H) 200](#_25lcl3g)

[PE-11 Emergency Power (M) (H) 201](#_kqmvb9)

[PE-12 Emergency Lighting (L) (M) (H) 202](#_34qadz2)

[PE-13 Fire Protection (L) (M) (H) 203](#_1jvko6v)

[PE-13 (2) Control Enhancement (M) (H) 203](#_43v86uo)

[PE-13 (3) Control Enhancement (M) (H) 204](#_2j0ih2h)

[PE-14 Temperature and Humidity Controls (L) (M) (H) 205](#_y5sraa)

[PE-14 (2) Control Enhancement (M) (H) 206](#_3i5g9y3)

[PE-15 Water Damage Protection (L) (M) (H) 206](#_1xaqk5w)

[PE-16 Delivery and Removal (L) (M) (H) 207](#_4hae2tp)

[PE-17 Alternate Work Site (M) (H) 208](#_2wfod1i)

[**13.12.**](#_1bkyn9b) **Planning (PL) 208**

[PL-1 Security Planning Policy and Procedures (L) (M) 208](#_3vkm5x4)

[PL-2 System Security Plan (L) (M) (H) 209](#_2apwg4x)

[PL-2 (3) Control Enhancement (M) (H) 211](#_pv6qcq)

[PL-4 Rules of Behavior (L) (M) 211](#_39uu90j)

[PL-4 (1) Control Enhancement (M) (H) 213](#_1p04j8c)

[PL-8 Information Security Architecture (M) (H) 213](#_48zs1w5)

[**13.13.**](#_2o52c3y) **Personnel Security (PS) 214**

[PS-1 Personnel Security Policy and Procedures (L) (M) 214](#_13acmbr)

[PS-2 Position Categorization (L) (M) 215](#_3na04zk)

[PS-3 Personnel Screening (L) (M) (H) 216](#_22faf7d)

[PS-3 (3) Control Enhancement (M) (H) 217](#_hkkpf6)

[PS-4 Personnel Termination (L) (M) 218](#_31k882z)

[PS-5 Personnel Transfer (L) (M) 219](#_1gpiias)

[PS-6 Access Agreements (L) (M) 220](#_40p60yl)

[PS-7 Third-Party Personnel Security (L) (M) 221](#_2fugb6e)

[PS-8 Personnel Sanctions (L) (M) 222](#_uzqle7)

[**13.14.**](#_3eze420) **Risk Assessment (RA) 223**

[RA-1 Risk Assessment Policy and Procedures (L) (M) 223](#_1u4oe9t)

[RA-2 Security Categorization (L) (M) (H) 224](#_2t9m75f)

[RA-3 Risk Assessment (L) (M) 225](#_18ewhd8)

[RA-5 Vulnerability Scanning (L) (M) (H) 226](#_27jua8u)

[RA-5 (1) Control Enhancement (M) (H) 228](#_mp4kgn)

[RA-5 (2) Control Enhancement (M) (H) 229](#_36os34g)

[RA-5 (3) Control Enhancement (M) (H) 229](#_1lu2dc9)

[RA-5 (5) Control Enhancement (M) (H) 230](#_45tpw02)

[RA-5 (6) Control Enhancement (M) (H) 231](#_2kz067v)

[RA-5 (8) Control Enhancement (L) (M) (H) 231](#_104agfo)

[**13.15.**](#_3k3xz3h) **System and Services Acquisition (SA) 232**

[SA-1 System and Services Acquisition Policy and Procedures (L) (M) 232](#_1z989ba)

[SA-2 Allocation of Resources (L) (M) (H) 233](#_4j8vrz3)

[SA-3 System Development Life Cycle (L) (M) (H) 234](#_2ye626w)

[SA-4 Acquisitions Process (L) (M) (H) 235](#_1djgcep)

[SA-4 (1) Control Enhancement (M) (H) 236](#_2coe5ab)

[SA-4 (2) Control Enhancement (L) (M) 237](#_rtofi4)

[SA-4 (8) Control Enhancement (M) (H) 238](#_3btby5x)

[SA-4 (9) Control Enhancement (M) (H) 239](#_1qym8dq)

[SA-4 (10) Control Enhancement (M) (H) 239](#_4ay9r1j)

[SA-5 Information System Documentation (L) (M) 240](#_2q3k19c)

[SA-8 Security Engineering Principles (M) (H) 241](#_158ubh5)

[SA-9 External Information System Services (L) (M) (H) 242](#_3p8hu4y)

[SA-9 (1) Control Enhancement (M) (H) 243](#_24ds4cr)

[SA-9 (2) Control Enhancement (M) (H) 244](#_jj2ekk)

[SA-9 (4) Control Enhancement (M) (H) 245](#_33ipx8d)

[SA-9 (5) Control Enhancement (M) (H) 245](#_1io07g6)

[SA-10 Developer Configuration Management (M) (H) 246](#_42nnq3z)

[SA-10 (1) Control Enhancement (M) (H) 247](#_2hsy0bs)

[SA-11 Developer Security Testing and Evaluation (M) (H) 248](#_wy8ajl)

[SA-11 (1) Control Enhancement (M) (H) 249](#_3gxvt7e)

[SA-11 (2) Control Enhancement (M) (H) 250](#_1w363f7)

[SA-11 (8) Control Enhancement (M) (H) 251](#_4g2tm30)

[**13.16.**](#_2v83wat) **System and Communications Protection (SC) 251**

[SC-1 System and Communications Protection Policy and Procedures (L) (M) 251](#_1ade6im)

[SC-2 Application Partitioning (M) (H) 252](#_3ud1p6f)

[SC-4 Information in Shared Resources (M) (H) 253](#_29ibze8)

[SC-5 Denial of Service Protection (L) (M) (H) 254](#_onm9m1)

[SC-6 Resource Availability (M) (H) 254](#_38n9s9u)

[SC-7 Boundary Protection (L) (M) (H) 255](#_1nsk2hn)

[SC-7 (3) Control Enhancement (M) (H) 256](#_47s7l5g)

[SC-7 (4) Control Enhancement (M) 257](#_2mxhvd9)

[SC-7 (5) Control Enhancement (M) (H) 258](#_122s5l2)

[SC-7 (7) Control Enhancement (M) (H) 258](#_3m2fo8v)

[SC-7 (8) Control Enhancement (M) (H) 259](#_217pygo)

[SC-7 (12) Control Enhancement (M) 260](#_4l7dh4h)

[SC-7 (13) Control Enhancement (M) 261](#_30cnrca)

[SC-7 (18) Control Enhancement (M) (H) 261](#_1fhy1k3)

[SC-8 Transmission confidentiality and Integrity (M) (H) 262](#_3zhlk7w)

[SC-8 (1) Control Enhancement (M) (H) 263](#_2emvufp)

[SC-10 Network Disconnect (M) 264](#_ts64ni)

[SC-12 Cryptographic Key Establishment & Management (L) (M) (H) 264](#_3drtnbb)

[SC-12 (2) Control Enhancement (M) (H) 265](#_1sx3xj4)

[SC-12 (3) Control Enhancement (M) (H) 266](#_4cwrg6x)

[SC-13 Use of Cryptography (L) (M) (H) 266](#_2s21qeq)

[SC-15 Collaborative Computing Devices (M) (H) 267](#_177c0mj)

[SC-17 Public Key Infrastructure Certificates (M) (H) 269](#_3r6zjac)

[SC-18 Mobile Code (M) (H) 269](#_26c9ti5)

[SC-19 Voice Over Internet Protocol (M) (H) 270](#_lhk3py)

[SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H) 271](#_35h7mdr)

[SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H) 272](#_1kmhwlk)

[SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H) 273](#_44m5f9d)

[SC-23 Session Authenticity (M) (H) 273](#_2jrfph6)

[SC-28 Protection of Information at Rest (M) (H) 274](#_ywpzoz)

[SC-28 (1) Control Enhancement (M) 275](#_3iwdics)

[SC-39 Process Isolation (L) (M) (H) 275](#_1y1nskl)

[**13.17.**](#_4i1bb8e) **System and Information Integrity (SI) 276**

[SI-1 System and Information Integrity Policy and Procedures (L) (M) 276](#_2x6llg7)

[SI-2 Flaw Remediation (L) (M) (H) 277](#_1cbvvo0)

[SI-2 (2) Control Enhancement (M) (H) 278](#_3wbjebt)

[SI-2 (3) Control Enhancement (M) (H) 279](#_2bgtojm)

[SI-3 Malicious Code Protection (L) (M) 280](#_qm3yrf)

[SI-3 (1) Control Enhancement (M) (H) 281](#_3alrhf8)

[SI-3 (2) Control Enhancement (M) (H) 281](#_1pr1rn1)

[SI-3 (7) Control Enhancement (M) (H) 282](#_49qpaau)

[SI-4 Information System Monitoring (L) (M) (H) 283](#_2ovzkin)

[SI-4 (1) Control Enhancement (M) (H) 284](#_1419uqg)

[SI-4 (2) Control Enhancement (M) (H) 285](#_3o0xde9)

[SI-4 (4) Control Enhancement (M) (H) 285](#_2367nm2)

[SI-4 (5) Control Enhancement (M) (H) 286](#_ibhxtv)

[SI-4 (14) Control Enhancement (M) (H) 287](#_32b5gho)

[SI-4 (16) Control Enhancement (M) (H) 288](#_1hgfqph)

[SI-4 (23) Control Enhancement (M) (H) 288](#_41g39da)

[SI-5 Security Alerts & Advisories (L) (M) (H) 289](#_2gldjl3)

[SI-6 Security Functionality Verification (M) (H) 290](#_vqntsw)

[SI-7 Software & Information Integrity (M) (H) 291](#_3fqbcgp)

[SI-7 (1) Control Enhancement (M) (H) 292](#_1uvlmoi)

[SI-7 (7) Control Enhancement (M) (H) 293](#_4ev95cb)

[SI-8 Spam Protection (M) (H) 293](#_2u0jfk4)

[SI-8 (1) Control Enhancement (M) (H) 294](#_195tprx)

[SI-8 (2) Control Enhancement (M) (H) 295](#_3t5h8fq)

[SI-10 Information Input Validation (M) (H) 295](#_28arinj)

[SI-11 Error Handling (M) (H) 296](#_ng1svc)

[SI-12 Information Output Handling and Retention (L) (M) (H) 297](#_37fpbj5)

[SI-16 Memory Protection (M) (H) 298](#_1mkzlqy)

[**14.**](#_46kn4er) **Acronyms 299**

[**SYSTEMS SECURITY PLAN ATTACHMENTS 300**](#_2lpxemk)

[**15.**](#_10v7oud) **Attachments 300**

[**Attachment 1**](#_4jzt0ds) **Information Security Policies and Procedures 301**

[**Attachment 2**](#_2z53all) **User Guide 302**

[**Attachment 3**](#_1eadkte) **Digital Identity Worksheet 303**

[Introduction and Purpose 303](#_3ya13h7)

[Information System Name/Title 303](#_2dfbdp0)

[Digital Identity Level Definitions 303](#_3ck96km)

[Review Maximum Potential Impact Levels 304](#_4bp6zg8)

[Digital Identity Level Selection 305](#_15zrjvu)

[**Attachment 4**](#_254pcrg) **PTA / PIA 306**

[Privacy Overview and Point of Contact (POC) 306](#_k9zmz9)

[Applicable Laws and Regulations 306](#_1jexfuv)

[Applicable Standards and Guidance 307](#_2ijv8qh)

[Personally Identifiable Information (PII) 307](#_3hot1m3)

[Privacy Threshold Analysis 308](#_1wu3btw)

[Qualifying Questions 308](#_4gtquhp)

[Designation 308](#_2vz14pi)

[**Attachment 5**](#_1b4bexb) **Rules of Behavior 309**

[**Attachment 6**](#_3v3yxl4) **Information System Contingency Plan 310**

[**Attachment 7**](#_2a997sx) **Configuration Management Plan 311**

[**Attachment 8**](#_peji0q) **Incident Response Plan 312**

[**Attachment 9**](#_39e70oj) **CIS Workbook 313**

[**Attachment 10**](#_1ojhawc) **FIPS 199 314**

[Introduction and Purpose 314](#_48j4tk5)

[Scope 314](#_2nof3ry)

[System Description 314](#_12tpdzr)

[Methodology 315](#_3mtcwnk)

[**Attachment 11**](#_h3xh36) **Separation of Duties Matrix 317**

[**Attachment 12**](#_313kzqz) **FedRAMP Laws and Regulations 318**

[**Attachment 13**](#_2fdt2ue) **FedRAMP Inventory Workbook 319**

**List of Figures**

[Figure 9-1 Authorization Boundary Diagram 10](#_2grqrue)

[Figure 9-2 Network Diagram 12](#_4f1mdlm)

[Figure 10-1 Data Flow Diagram 14](#_3tbugp1)

**List of Tables**

[Table 1-1. Information System Name and Title 1](#_tyjcwt)

[Table 2-1. Security Categorization 1](#_1t3h5sf)

[Table 2-2. Sensitivity Categorization of Information Types 3](#_2s8eyo1)

[Table 2-3. Security Impact Level 3](#_3rdcrjn)

[Table 2-4. Baseline Security Configuration 4](#_26in1rg)

[Table 3-1. Information System Owner 4](#_1ksv4uv)

[Table 5-1. Information System Management Point of Contact 5](#_z337ya)

[Table 5-2. Information System Technical Point of Contact 5](#_1y810tw)

[Table 6-1. CSP Name Internal ISSO (or Equivalent) Point of Contact 6](#_2xcytpi)

[Table 6-2. AO Point of Contact 6](#_1ci93xb)

[Table 7-1. System Status 7](#_2bn6wsx)

[Table 8-1. Service Layers Represented in this SSP 8](#_49x2ik5)

[Table 8-2. Cloud Deployment Model Represented in this SSP 9](#_147n2zr)

[Table 8-3. Leveraged Authorizations 9](#_23ckvvd)

[Table 9-1. Personnel Roles and Privileges 11](#_3fwokq0)

[Table 10-1 Ports, Protocols and Services 15](#_nmf14n)

[Table 11-1. System Interconnections 16](#_46r0co2)

[Table 12-1. Information System Name Laws and Regulations 18](#_3l18frh)

[Table 12-2. Information System Name Standards and Guidance 19](#_4k668n3)

[Table 13-1. Summary of Required Security Controls 19](#_1egqt2p)

[Table 13-2. Control Origination and Definitions 25](#_3ygebqi)

[Table 13-3. CA-3 Authorized Connections 86](#_1smtxgf)

[Table 15-1. Names of Provided Attachments 300](#_2005hpz)

[Table 15-2. Information System Name and Title 303](#_sklnwt)

[Table 15-3. Mapping FedRAMP Levels to NIST SP 800-63-3 Levels 304](#_1rpjgsf)

[Table 15-4. Potential Impacts for Assurance Levels 305](#_2quh9o1)

[Table 15-5. Digital Identity Level 305](#_3pzf2jn)

[Table 15-6. - Information System Name; Privacy POC 306](#_349n5n2)

[Table 15-7. <Information System Name> Laws and Regulations 307](#_43ekyio)

[Table 15-8. <Information System Name> Standards and Guidance 307](#_xp5iya)

[Table 15-9. CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1 316](#_21yn6vd)

**System Security Plan Approvals**

Cloud Service Provider Signatures

|  | | | | |
| --- | --- | --- | --- | --- |
| Name | <Enter Name> | | Date | <Select Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | CSP Name | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | <Enter Name> | | Date | <Select Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | CSP Name | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | <Enter Name> | | Date | <Select Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | CSP Name | | |
|  | |  | | |

# Information System Name/Title

This System Security Plan provides an overview of the security requirements for the Information System Name (Enter Information System Abbreviation) 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 the Enter Information System Abbreviation information system.

The security safeguards implemented for the Enter Information System Abbreviation 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** |
| --- | --- | --- |
| <Enter FedRAMP Application Number> | Information System Name | Enter Information System Abbreviation |

# 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:** | Moderate |
| --- | --- |

## 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 Enter Information System Abbreviation. 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.

*Instruction: Record your information types in the tables that follow. Record the sensitivity level for Confidentiality, Integrity and Availability as High, Moderate, or Low. Add more rows as needed to add more information types. Use NIST SP 800-60 Guide for Mapping Types of Information and Systems to Security Categories, Volumes I & II, Revision 1 for guidance.*

*Delete this instruction from your final version of this document.*

Example:

| **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 | Moderate | Low |

*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** |
| --- | --- | --- | --- | --- |
| <Enter Information Type> | <Enter NIST Identifier> | Choose level. | Choose level. | Choose level. |
| <Enter Information Type> | <Enter NIST Identifier> | Choose level. | Choose level. | Choose level. |
| <Enter Information Type> | <Enter NIST Identifier> | Choose level. | Choose level. | Choose level. |

## Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2-2 Sensitivity Categorization of Information Types, for the Enter Information System Abbreviation, 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** | Moderate |
| **Integrity** | Moderate |
| **Availability** | Moderate |

Through review and analysis, it has been determined that the baseline security categorization for the Enter Information System Abbreviation system is listed in the Table 2-4 Baseline Security Configuration that follows.

*Table 2-4. Baseline Security Configuration*

| **Enter Information System Abbreviation Security Categorization** | Choose level |
| --- | --- |

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 Choose an item.

Additional digital identity information can be found in Section 15 Attachments Digital Identity Level Selection.

# 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** | <Enter Name> |
| **Title** | <Enter Title> |
| **Company / Organization** | <Enter Company/Organization>. |
| **Address** | <Enter Address, City, State and Zip> |
| **Phone Number** | <555-555-5555> |
| **Email Address** | <Enter email address> |

# Authorizing Official

*Instruction: The Authorizing Official is determined by the path that the CSP is using to obtain an authorization.*

*JAB P-ATO: FedRAMP, JAB, as comprised of member representatives from the General Services Administration (GSA), Department of Defense (DoD) and Department of Homeland Security (DHS)*

*Agency Authority to Operate (ATO): Agency Authorizing Official name, title and contact information*

*Delete this and all other instructions from your final version of this document.*

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the *Insert AO information as instructed above*.

# Other Designated Contacts

*Instruction: AOs should use the following section to identify points of contact that understand the technical implementations of the identified cloud system. AOs should edit, add, or modify the contacts in this section as they see fit.*

*Delete this and all other instructions from your final version of this document.*

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

*Table 5-2. Information System Technical Point of Contact*

| **Information System Technical Point of Contact** | |
| --- | --- |
| **Name** | <Enter Name> |
| **Title** | <Enter Title> |
| **Company / Organization** | <Enter Company/Organization>. |
| **Address** | <Enter Address, City, State and Zip> |
| **Phone Number** | <555-555-5555> |
| **Email Address** | <Enter email address> |

*Instruction: Add more tables as needed.*

*Delete this and all other instructions from your final version of this document.*

| **Point of Contact** | |
| --- | --- |
| **Name** | <Enter Name> |
| **Title** | <Enter Title> |
| **Company / Organization** | <Enter Company/Organization>. |
| **Address** | <Enter Address, City, State and Zip> |
| **Phone Number** | <555-555-5555> |
| **Email Address** | <Enter email address> |

# 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. CSP Name Internal ISSO (or Equivalent) Point of Contact*

| **CSP Name Internal ISSO (or Equivalent) Point of Contact** | |
| --- | --- |
| **Name** | <Enter Name> |
| **Title** | <Enter Title> |
| **Company / Organization** | <Enter Company/Organization>. |
| **Address** | <Enter Address, City, State and Zip> |
| **Phone Number** | <555-555-5555> |
| **Email Address** | <Enter email address> |

*Table 6-2. AO Point of Contact*

| **AO Point of Contact** | |
| --- | --- |
| **Name** | <Enter Name> |
| **Title** | <Enter Title> |
| **Organization** | <Enter Company/Organization>. |
| **Address** | <Enter Address, City, State and Zip> |
| **Phone Number** | <555-555-5555> |
| **Email Address** | <Enter email address> |

# 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: Click here to enter text. |

*Instruction: Select as many status indicators as apply. If more than one status is selected, list which components of the system are covered under each status indicator.*

*Delete this and all other instructions from your final version of this document.*

# Information System Type

The Enter Information System Abbreviation 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 the Enter Information System Abbreviation defined in this SSP are indicated in Table 8-1 Service Layers Represented in this SSP that follows.

*Instruction: Check all layers that apply.*

*Delete this and all other instructions from your final version of this document.*

*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: Click here to enter text. |

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 the Enter Information System Abbreviation 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.

*Instruction: Check deployment model that applies.*

*Delete this and all other instructions from your final version of this document.*

*Table 8-2. Cloud Deployment Model Represented in this SSP*

| **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)  Click here to enter text. |

## Leveraged Authorizations

*Instruction: The FedRAMP program qualifies different service layers for Authorizations. One or multiple service layers can be qualified in one System Security Plan. If a lower level layer has been granted an Authorization and another higher-level layer represented by this SSP plans to leverage a lower layer’s Authorization, this System Security Plan must clearly state that intention. If an information system does not leverage any pre-existing Authorizations, write “None” in the first column of the table that follows. Add as many rows as necessary in the table that follows.*

*Delete this and all other instructions from your final version of this document.*

The Enter Information System Abbreviation Choose an item leverages a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by this Enter Information System Abbreviation 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** |
| --- | --- | --- |
| <Enter Leveraged information system name1> | <Enter service provider owner1> | <Date> |
| <Enter Leveraged information system name2> | <Enter service provider owner2> | <Date> |
| <Enter Leveraged information system name3> | <Enter service provider owner3> | <Date> |

# General System Description

This section includes a general description of the Enter Information System Abbreviation.

## System Function or Purpose

*Instruction: In the space that follows, describe the purpose and functions of this system.*

*Delete this and all other instructions from your final version of this document.*

## Information System Components and Boundaries

*Instruction: In the space that follows, provide an explicit definition of the system’s Authorization Boundary. Provide a diagram that portrays this Authorization Boundary and all its connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system. Address all components and managed interfaces of the information system authorized for operation (e.g., routers, firewalls).*

*The diagram must include a predominant border drawn around all system components and services included in the authorization boundary. The diagram must be easy to read and understand.*

*Formal names of components as they are known at the service provider organization in functional specifications, configuration guides, other documents and live configurations shall be named on the diagram and described. Components identified in the Boundary diagram should be consistent with the Network diagram and the inventory(ies). Provide a key to symbols used. Ensure consistency between the boundary and network diagrams and respective descriptions (Section 9.4) and the appropriate Security Controls [AC-20, CA-3(1)].*

***Additional FedRAMP Requirements and Guidance:***

***Guidance:*** *See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> FedRAMP Authorization Boundary Guidance*

[*https://www.fedramp.gov/documents/*](https://www.fedramp.gov/documents/)

*Delete this and all other instructions from your final version of this document.*

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9-1 Authorization Boundary Diagram below.

|  |
| --- |

*Figure 9-1 Authorization Boundary Diagram*

## 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.

*Instruction: For an External User, write “Not Applicable” in the Sensitivity Level Column. This table must include all roles including systems administrators and database administrators as a role types. (Also include web server administrators, network administrators and firewall administrators if these individuals have the ability to configure a device or host that could impact the CSP service offering.)*

*This table must also include whether these roles are fulfilled by foreign nationals or systems outside the United States.*

*Delete this and all other instructions from your final version of this document.*

*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** |
| --- | --- | --- | --- | --- | --- |
| UNIX System Administrator | Internal | P | Moderate | Full administrative access (root) | Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups |
| Client Administrator | External | NP | N/A | Portal administration | Add/remote client users. Create, modify and delete client applications |
| Program Director | Internal | NLA | Limited | N/A | Reviews, approves and enforces policy |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |

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

## Network Architecture

*Instruction: Insert a network architectural diagram in the space that follows. Ensure that the following items are labeled on the diagram: hostnames, Domain Name System (DNS) servers, DHCP servers, authentication and access control servers, directory servers, firewalls, routers, switches, database servers, major applications, storage, Internet connectivity providers, telecom circuit numbers, network interfaces and numbers, VLANs. Major security components should be represented. If necessary, include multiple network diagrams.*

*Delete this and all other instructions from your final version of this document.*

Assessors should be able to easily map hardware, software and network inventories back to this diagram.

The logical network topology is shown in Figure 9-2 Network Diagram mapping the data flow between components.

The following Figure 9-2 Network Diagram(s) provides a visual depiction of the system network components that constitute Enter Information System Abbreviation.

|  |
| --- |

*Figure 9-2 Network Diagram*

# System Environment And Inventory

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

*Instruction: In the space that follows, provide a general description of the technical system environment. Include information about all system environments that are used, e.g., production environment, test environment, staging or QA environments. Include the specific location of the alternate, backup and operational facilities.*

*In your description, also include a reference to Attachment 13, the system’s Integrated Inventory Workbook, which should provide a complete listing of the system’s components (operating systems/infrastructure, web applications/software, and databases). The Integrated Inventory Workbook should be maintained and updated monthly by the CSP, as part of continuous monitoring efforts. Instructions for completing the Integrated Inventory Workbook are provided within the Integrated Inventory Workbook.*

*Delete this and all other instructions from your final version of this document.*

## Data Flow

*Instruction: In the space that follows, describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. Include data flows for privileged and non-privileged authentication/authorization to the system for internal and external users. If necessary, include multiple data flow diagrams.*

*Delete this and all other instructions from your final version of this document.*

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*

## Ports, Protocols and Services

Table 10-1 Ports, Protocols and Services below lists the ports, protocols and services enabled in this information system.

*Instruction: In the column labeled “Used By” please indicate the components of the information system that make use of the ports, protocols and services. In the column labeled “Purpose” indicate the purpose for the service (e.g., system logging, HTTP redirector, load balancing). This table should be consistent with CM-6 and CM-7. You must fill out this table, even if you are leveraging a pre-existing FedRAMP Authorization. Add more rows as needed.*

*Delete this and all other instructions from your final version of this document.*

*Table 10-1 Ports, Protocols and Services*

| **Ports (TCP/UDP)\*** | **Protocols** | **Services** | **Purpose** | **Used By** |
| --- | --- | --- | --- | --- |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |

\* Transmission Control Protocol (TCP), User Diagram Protocol (UDP)

# System Interconnections

*Instruction: List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the CSP system that provides the connection. Name the external organization and the IP address of the external system. Provide a point of contact and phone number for the external organization. For Connection Security indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed. This table must be consistent with Table 13-3 CA-3 Authorized Connections.*

***Additional FedRAMP Requirements and Guidance:***

***Guidance:*** *See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> FedRAMP Authorization Boundary Guidance*

[*https://www.fedramp.gov/documents/*](https://www.fedramp.gov/documents/)

*Delete this and all other instructions from your final version of this document.*

The 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** |
| --- | --- | --- | --- | --- | --- | --- |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |

\*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 Information System Name Laws and Regulations includes additional laws and regulations specific to Information System Name.

*Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the CSP does not have additional laws and regulations that it must follow, please specify "N/A" in the table.*

*Delete this and all other instructions from your final version of this document.*

*Table 12-1. Information System Name Laws and Regulations*

| **Identification Number** | **Title** | **Date** | **Link** |
| --- | --- | --- | --- |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |

## Applicable Standards and Guidance

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

Table 12-2 Information System Name Standards and Guidance includes in this section any additional standards and guidance specific to Information System Name.

*Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the CSP does not have additional standards or guidance that it must follow, please specify "N/A" in the table.*

*Delete this and all other instructions from your final version of this document.*

*Table 12-2. Information System Name Standards and Guidance*

| **Identification Number** | **Title** | **Date** | **Link** |
| --- | --- | --- | --- |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |

# 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 Enter Information System Abbreviation 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 |
| **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) |
| **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) |
| **IR** | **Incident Response** | | | | |
| **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.

*Instruction: In the sections that follow, describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage and monitor the control. In some cases, the responsibility is shared by a CSP and by the customer. Use the definitions in the table that follows to indicate where each security control originates from.*

*Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.*

*For SaaS and PaaS systems that are inheriting controls from an IaaS (or anything lower in the stack), the “inherited” check box must be checked and the implementation description must simply say “inherited.” FedRAMP reviewers will determine whether the control-set is appropriate or not.*

*In Section 13, the NIST term "organization defined" must be interpreted as being the CSP's responsibility unless otherwise indicated. In some cases the JAB has chosen to define or provide parameters, in others they have left the decision up to the CSP.*

*Please note: CSPs should not modify the control requirement text, including the parameter assignment instructions and additional FedRAMP requirements. CSP responses must be documented in the “Control Summary Information” and “What is the solution and how is it implemented?” tables.*

*Delete this and all other instructions from your final version of this document.*

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 CSP Name 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 the CSP Name 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 CSP Name. | 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 CSP Name 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 CSP Name 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 (L) (M)

The organization:

1. Develops, documents and disseminates to [*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

Reviews and updates the current:

* 1. Access control policy [*FedRAMP Assignment: at least every 3 years*]; and
  2. Access control procedures [*FedRAMP Assignment: at least annually*].

| **AC-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Security Specialist | |
| Parameter AC-1(a): Security Specialist | |
| Parameter AC-1(b)(1): 3 years | |
| Parameter AC-1(b)(2): Annually | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **AC-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | The company assigns authorized administrators who are responsible for giving access , deleting profiles, updating roles to users etc. Admin gives role and access to users based on their job roles and groups.To guarantee the efficiency of the policy and compliance with security requirements, regular audits, evaluations, and modifications are carried out. |
| **Part b1** | There is an administrator head who is responsible for getting policy reviewed and updated in the organization. We evaluate and update our policy every so often to maintain the continuous security and compliance for our organization. In accordance with FedRAMP specifications, this procedure is required to take place at least every three years.When the evaluation is complete and the policy has been changed, the admin head will share it with the entire team and all stakeholders. |
| **Part b2** | The access control policy and related procedures are shared with all the IT manager admin and system administrators. This dissemination is done through our internal portal and training sessions, ensuring that all stakeholders are well-informed about access control measures. |

### AC-2 Account Management (L) (M)

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:
9. When accounts are no longer required;
10. When users are terminated or transferred; and
11. When individual information system usage or need-to-know changes;
12. 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;
13. Reviews accounts for compliance with account management requirements [*FedRAMP Assignment: at least annually*]; and
14. 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: IT Manager/Administrator – Responsible for Account Management | |
| Parameter AC-2(a): The company uses Amazon IAM for system account(s). | |
| Parameter AC-2(e): The company assigns L1/HR Managers to approve requests for new users in the system. | |
| Parameter AC-2(f): Sentinel Shield Account Management Policy. | |
| Parameter AC-2(j): Every (1) year(s). | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | The company uses Amazon IAM to manage system accounts. Amazon Web Services is the external service used for creating, managing, and deleting old and new system accounts. |
| **Part b** | The company assigns an account manager, an IT department lead who has administrative access to the IAM platform. No one else in the organization is allowed to access the IAM platform for managing system accounts except for the IT department lead, authorized System Administrators and authorized IT specialist who are in charge of creating and managing (system) accounts. |
| **Part c** | The same as part b; The Company assigns an account manager (IT department lead) who is in charge of creating and managing accounts as well as managing the account roles that are part of our system (i.e. membership roles). |
| **Part d** | The company assigns authorized administrators and users to manage the role and access authorizations of other users and employees. Besides having managers, there can be IT Administrators, System Administrators (who have access to control most user systems; change roles and add/delete accounts) and IT Authorized Specialists who may have special access to view and report on IAM user data. |
| **Part e** | To create new accounts authorization from the respective reporting manager is required to initiate the process. (i.e. L1 managers) |
| **Part f** | Administrators have access to create, modify and delete accounts. Whenever an operator in the company leaves, an admin has the authority to disable or delete those accounts so that they can no longer access the system. These actions will be done with the approval of the authorized managers and the respective account administrator can then perform the required action needed. |
| **Part g** | The company uses Cloud Watch for monitoring the audit logs which is essential and can help to keep track of the account activity and ensure compliance. Each administrator has access to a set of accounts where he can monitor the activities. |
| **Part h** | The accounts that are no longer needed are subsequently removed after the IT department lead is notified and when the approval is given. When the users are transferred from one unit to another, separate login data credentials are created by the administrators automatically. When users are terminated, the administrators can delete the accounts which are associated with the users. In case of the need-to-know changes, the administrators are notified and depending on the severity, the actions are taken by the administrators. |
| **Part i** | Firstly, the company verifies an individual's identity and confirms their access authorization. Then we also ensure that person is given only the required to relevant sections of the system. The company checks for organizational attributes, such as duration, geographic, time-based restrictions, and then further refine permissions as well. |
| **Part j** | The company uses AWS IAM roles which automatically tracks and reports user activity. which includes the last login details of each user and also ensures that there is multi factor authentication and validating the permissions aligned to the defined user role. |
| **Part k** | When the person in a certain department leaves, the IT department is notified and they identify the person's group account. The credentials of these accounts are then changed inorder to maintain security. Also once the credentials are changed the members of the group are informed with the updated credentials ensuring that the credentials remain confidential. All the changes are logged for future periodic audit checks. |

#### 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: IT Administrator | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-2 (1) What is the solution and how is it implemented?** |
| --- |
| The company (Sentinel Shield) has several automations using Amazon IAM to create, modify and delete users depending on the action and/or activity of a user (which also includes employees). An example of such automation is: a request for a user to be added onto a system is approved by upper management (L1 managers and/or HR manager(s)), once that’s approved through our system it triggers a user to be created in Amazon IAM. Once created in IAM, a user is assigned default roles and permissions (basic access to systems) for which the IT administrator or authorized System Administrator assigns roles and permissions based on their requirements. |

#### AC-2 (2) Control Enhancement (M)

The information system automatically [*Selection: removes; disables*] temporary and emergency accounts after [*FedRAMP Assignment: no more than 30 days for temporary and emergency account types*].

| **AC-2 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: IT Administrator or Authorized System Administrator | |
| Parameter AC-2(2)1: Disables | |
| Parameter AC-2(2)2: 30 Days | |
| Implementation Status (check all that apply):   * Implemented * Partially implemented * Planned * Alternative implementation * Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-2 (2) What is the solution and how is it implemented?** |
| --- |
| Any temporary and/or emergency account created in our system, it’s disabled after a period of 30 days. This period of time gives the developer or employee time to make use of the account for certain types of testing (e.g. rolling out a new feature and the software development lead wants to try it out using a temporary user account). Emergency accounts can be used when a security incident has happened (e.g. an administrator account was compromised and a manager/IT administrator can use an Emergency Account to shut systems down and/or prevent further incidents). |

#### AC-2 (3) Control Enhancement (M)

The information system automatically disables inactive accounts after [*FedRAMP Assignment: ninety (90) 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 Joint Authorization Board (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: IT Administrator or Authorized System Administrator | |
| Parameter AC-2(3): 90 Days | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-2 (3) What is the solution and how is it implemented** |
| --- |
| User accounts that are inactive after 90 days are automatically inactivated by the Amazon IAM system. Accounts can also be inactivated/disabled prior to this timeframe for any given reason by an authorized administrator. The automated action to inactivate accounts does not require upper management approval, it’s based on our policy. This inactivation includes non-management/operation users. Account inactivation does not equal deletion, if a user decides to come back or is approved to come back for any reason, their access will be re-activated. |

#### AC-2 (4) Control Enhancement (M)

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [*Assignment: organization-defined personnel or roles*].

| **AC-2 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: IT Administrator | |
| Parameter AC-2(4): creation, modification, enabling, disabling, removal, notifies | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-2 (4) What is the solution and how is it implemented?** |
| --- |
| The company uses the amazon IAM account services to manage all the accounts automatically and audit them on time intervals, respective account administrators will monitor these audits for any inconsistencies, manual audits would be also done in time intervals to verify automated audit results. Any red flag highlighted in the automated audit will notify the respective account manager and account admin. |

#### AC-2 (5) Control Enhancement (M)

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

**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: Account user | |
| Parameter AC-2(5): Automated log out based on inactivity | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-2 (5) What is the solution and how is it implemented?** |
| --- |
| The account users would be logged out of their accounts after a time of inactivity which is defined in the organization rules. The Account management system IAM is predefined in a way to do these tasks automatically and the rules are monitored by the IT admins. |

#### AC-2 (7) Control Enhancement (M)

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;

(b) Monitors privileged role assignments; and

Takes [*Assignment: organization-defined actions*] when privileged role assignments are no longer appropriate.

| **AC-2 (7)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: IT Administrator | |
| Parameter AC-2(7)(c): role based access | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-2 (7) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | The company utilizes a role-based access control (RBAC) system to categorize and administer privileged user accounts. Each privileged role, like "System Administrator" or "Database Administrator", is assigned specific system access based on necessity. Automated tools monitor these privileged activities in real-time, alerting on any unusual actions. If a privileged role is found inappropriate, the account will be suspended, reviewed, and either reassigned or revoked. Any changes made are clearly documented and communicated to the account holder. |
| **Part b** | The IAM monitors privileged role assignments using sophisticated monitoring tools, ensuring all actions undertaken by privileged users align with their roles. |
| **Part c** | The company revokes the account access when privileged role assignments are no longer appropriate, these are taken care of by the automated account services IAM, these tasks will be monitored by the respective IT administrators to make sure no gaps are there. |

#### AC-2 (9) Control Enhancement (M)

The organization only permits the use of shared/group accounts that meet [*Assignment: organization-defined conditions for establishing shared/group accounts*].

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

| **AC-2 (9)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: IT Administrator | |
| Parameter AC-2(9): | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-2 (9) What is the solution and how is it implemented?** |
| --- |
| It is ensured that the organization only allowed the utilization of shared/group accounts that adhered to predefined conditions established by the organization. The objective is to maintain a robust access control framework and prevent unauthorized use of shared/group accounts. Comprehensive documentation outlining the organization's conditions for establishing shared/group accounts, including the rationale behind each condition has been developed to ensure the better distinction. |

#### 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: IT administrators | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-2 (10) What is the solution and how is it implemented?** |
| --- |
| User account management is facilitated through Amazon IAM. The company has established a comprehensive user account lifecycle management process using IAM. This process involves the creation, modification, and deletion of users, aligning with the project's security and access control policies. When members leave their respective groups or roles within the organization, the IT administrators are responsible for initiating the termination process of their credentials. This includes revoking access to AWS resources by modifying or deleting their IAM permissions. |

#### AC-2 (12) Control Enhancement (M)

The organization:

1. Monitors information system accounts for [*Assignment: organization-defined atypical use*]; and

Reports atypical usage of information system accounts to [*Assignment: organization-defined personnel or roles*].

**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: IT Administrator/System Administrator | |
| Parameter AC-2(12)(a): IT Administrator/System Administrator | |
| Parameter AC-2(12)(b): CSO (Chief Security Officer) | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-2 (12) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | The IT Administrator is in charge of monitoring all the different services pertaining information systems as well as any security, access and role systems. An IT Administrator is in charge of monitoring and reporting to the CSO as well if there’s any type of incident. An IT Administrator is in charge of incident reporting as well as assigning fixes to any occurring incidents. |
| **Part b** | The CSO (Chief Security Officer) will be reported on such incidents and report to other upper level staff depending on severity. The CSO will then also be in charge of directing the IT Administrator on which incident to report or act on (if there’s multiple incidents). |

### 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: | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-3 What is the solution and how is it implemented?** |
| --- |
| Along with AWS IAM for role and user access, every user is given certain roles that will affect their system-wide access. Not every type of user has access to the same parts of our information system. This system is heavily secured using AWS IAM permissions along with 2-Factor Authentication. Any account that fails to login after 4 different tries, is automatically deactivated. This is because our information system contains a lot of highly critical data which only authorized users are allowed to access. |

### 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: CSO (Chief Security Officer) | |
| Parameter AC-4: Sentinel Shield Security Policy | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-4 What is the solution and how is it implemented?** |
| --- |
| The information system is controlled through policies described in the “Sentinel Shield Security Policy” document. This document describes all of the enforced security policies for Sentinel Shield services in heavy detail. This document is reviewed annually to keep policies up to date. If there’s a critical issue regarding security (network and/or system security), the document will be promptly reviewed, updated and enforced through the different layers of our information system. The information system flow is managed by the CSO (Chief Security Officer), who is in charge of its system structure and design, as well as enforcing its policies against the different types of departments that fall under it. |

#### 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: IT Administrator/System Administrator | |
| Parameter AC-4(21)-1: AWS IAM along with custom network functions (e.g. firewalls), that provide ways to control who is allowed in a certain network (or subnet) and/or system. | |
| Parameter AC-4(21)-2: Sentinel Shield Security Policies | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-4 (21) What is the solution and how is it implemented?** |
| --- |
| The information system is partitioned into different layers for the purpose of security. Each layer has a different severity role (i.e. each level contains different types of non-critical or critical data). Each layer in the system is protected through several steps of security, which includes: AWS IAM for system roles and authentication, (virtualized) network functions with integrated role verification for controlling access and traffic, and custom code for authentication into the internal subsystems within the layer you’re authenticated for.  The network functions that control access for these systems play a critical role for our security. These network functions are highly maintained and managed by the IT Administrator and System Administrator. They need to ensure that there is no downtime between services. If there is any downtime, it needs to ensure that it protects and shuts down system-wide information services so it doesn’t cause a security vulnerability. |

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

The organization:

1. Separates [*Assignment: organization-defined duties of individuals*];
2. Documents separation of duties of individuals; and
3. 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: COO (Chief Operations Officer) | |
| Parameter AC-5(a): System-wide business planning and corporate role assignment(s) | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | The COO is responsible for (internal) system-wide planning as well as system-wide organization structure to define the roles of the company. The COO plays a very important role as they define the needs for the company and assign the correct amount of workforce to the different departments. The COO is not responsible for assigning the sub-teams and/or sub-departments, which are managed by the department heads. Although, depending on what type of system critical information those employees in the sub-departments might be working on, the department head will need to gain approval of the COO alongside the CSO to give access to those employees. |
| **Part b** | This separation of individuals is also handled mainly by the COO. The COO can assign department heads (i.e. head of Engineering, IT Administrator, Security Administrator, etc.). Although, those department heads have a say in who’s going to be working under them in their team, which separates concerns from the COO to the department head level. |
| **Part c** | The COO is in charge of internal system-wide access authorizations. Since the COO is in charge of handling the internal business, planning and operations affairs of the company, they’re also in charge of authorizing which departments (and sub-departments) get what type of access. The COO works in conjunction with the CSO (Chief Security Officer) to achieve this goal. Both the COO and the CSO are important in this step since they help define the high-level security measures that need to be taken for each department and sub-department if needed; the head of each department can assign sub-department authorizations (e.g. the IT Administrator assigning auth. access to a team of DevOps engineers in another team under IT/Engineering). |

### 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: | |
| Implementation Status (check all that apply):   * Implemented * Partially implemented * Planned * Alternative implementation * Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate * Service Provider System Specific * Service Provider Hybrid (Corporate and System Specific) * Configured by Customer (Customer System Specific) * Provided by Customer (Customer System Specific) * Shared (Service Provider and Customer Responsibility) * Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-6 What is the solution and how is it implemented?** |
| --- |
| In order to keep the system secure, we follow a least privilege rule which means that we only give people the access and permissions they absolutely need to do their job. So this helps to keep things secure, lowering the risk of any security issues. We also, manage this through a system where roles are clearly defined. Moreover, there are two main types of administrators in our setup :   1. System Administrators : These folks take care of the technical side, making sure everything runs smoothly and securely on the IT front. 2. Executive Administrators : They focus on the business side of things, ensuring each department has just the right level of access to get their jobs done without any extra permissions that could potentially be misused.   We review these roles regularly, at least twice a year and make sure everything is in order and update as necessary and mainly if there are significant changes in our team or how we operate. Also, we make sure to improve our systems further with well defined plans and guidelines that show exactly how we are keeping data safe and secure as per FedRAMP standards. |

#### AC-6 (1) Control Enhancement (M)

The organization explicitly authorizes access to [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*].

| **AC-6 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter AC-6(1): | |
| Implementation Status (check all that apply):   * Implemented * Partially implemented * Planned * Alternative implementation * Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate * Service Provider System Specific * Service Provider Hybrid (Corporate and System Specific) * Configured by Customer (Customer System Specific) * Provided by Customer (Customer System Specific) * Shared (Service Provider and Customer Responsibility) * Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-6 (1) What is the solution and how is it implemented?** |
| --- |
| According to the strong security policy we defined, we have also implemented strict protocols inorder to regulate access to critical security functionalities and sensitive data that is present in the system's hardware, software, and firmware. This initiative is managed by theInformation Security Officer, who clearly outlines the access privileges, ensuring that only authorized individuals have access to vital security information and functions. This approach not only defines who can access such critical data but also closely monitors the extent of the access granted, preventing any unauthorized usage. Our team also maintains vigilance through regular audits and adjusts protocols as needed ensuring continuous alignment with FedRAMP's high security standards. Through this way we can constantly protect the organization's valuable data assets while promoting a secure and responsible working environment. |

#### 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: | |
| Parameter AC-6(2): | |
| Implementation Status (check all that apply):   * Implemented * Partially implemented * Planned * Alternative implementation * Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate * Service Provider System Specific * Service Provider Hybrid (Corporate and System Specific) * Configured by Customer (Customer System Specific) * Provided by Customer (Customer System Specific) * Shared (Service Provider and Customer Responsibility) * Inherited from pre-existing FedRAMP Authorization for Date of Authorization , | |

| **AC-6 (2) What is the solution and how is it implemented?** |
| --- |
| To keep the system safe we came with a policy where users with access to security functions must use non-privileged accounts when accessing non-security functions. This policy, under the supervision of the Security Manager prevents potential misuse of access rights and maintains the integrity of our secure data and functions. Our implementation process is straightforward and critical, with configurations that limit non-security access to non-privileged accounts only. Clear guidelines are established so that the security functions and the confines of each role. Regular updates and reviews are conducted to maintain alignment with FedRAMP standards which ensures that our operational environment remains secure and responsible at all times. |

#### 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: Information security officer / IT Admin | |
| Parameter AC-6 (5): | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-6 (5) What is the solution and how is it implemented?** |
| --- |
| The account users are able to do only activities or access the information which they are privileged to only, This access control is managed by the PAM which is a subset of AWS. The company provides access to only to the accounts which are meant to do the critical tasks, therfore only privileged accounts will be able to perform such tasks. This isolation helps in un-priviliged accounts to no gain access to sensitive information and prevents unauthorized activities. Each account will be assigned privileges based on the role they are in and additional previliges may be given at the permission of IT admin/ reporting manager / IS officer. |

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

The information system audits the execution of privileged functions.

| **AC-6 (9)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Information security officer / IT Admin | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-6 (9) What is the solution and how is it implemented?** |
| --- |
| The solution for execution of privileged functions is given via privileged access manager(PAM) which is a subset of the AWS. PAM helps us to maintain the access control for every usecase and limits the unwanted users from doing unauthorized activities. The PAM has privilege account management, privilege access management and event management which helps us to monitor all the activities done/ doing by the account users. The PAM solution is implemented via the cloud in which helps the company in avoiding on premise setup costs. PAM has helped in maintaining the privilege accounts and categorizing them based on the admin rules. The PAM also supports the account activity which gives insights about all the activity done and alerts the users if there is any unauthorized activity being done. |

#### 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: Information Security Officer / IT Admin | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-6 (10) What is the solution and how is it implemented?** |
| --- |
| The PAM(Previliged access management) is implemente to maintain the non-previliged members from executing the privileged functions. The PAM is maintained by the ISO/ IT Admin who would limit the accounts previliges based on their activities which inturns helps to avoid the non privileged user to execute privileged functions. In addition to the PAM the company also manually verifies the privilege access information to ensure everyting is in right place. company also monitors the access control violations in order to take required corrective actions. |

### AC-7 Unsuccessful Login Attempts (L) (M)

The organization:

1. 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

(b) Automatically [*Selection: locks the account/node for a* [*FedRAMP Assignment: thirty (30) minutes*]; *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: System Administrators | |
| Parameter AC-7(a)-1: Consecutive Invalid logins | |
| Parameter AC-7(a)-2: Failure Logins counts in 15 minutes time frame. | |
| Parameter AC-7(b)-1: Automatically locks the account for 15 mins | |
| Parameter AC-7(b)-2: Delays the next log on prompt. | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-7 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | We use AWS Identity and Access Management (IAM) in our backend architecture to set limitations on the number of consecutive failed login attempts and the time period during which these attempts are taken into account. We have created an IAM policy that prohibits users from making more than three unsuccessful login attempts within a 15-minute period in order to strengthen the security of our application. In the event that such occurrences do take place, we immediately provide our system administrator with thorough details so they can take appropriate action. The system administrator then block the user's profile for 24 hours and keeps a close eye on login activity during that period. |
| **Part b** | A policy for account lockouts has been implemented to restrict the number of failed login attempts. Once the maximum allowed unsuccessful login attempts are reached, the subsequent login prompt is delayed by 15 minutes. Depending on specific criteria, user accounts may be subsequently locked, and notifications are sent to system administrators. AWS CloudTrail is configured to capture logs related to authentication and access events. In the event of an account being locked due to multiple failed login attempts, automated alerts are dispatched to system administrators or security personnel. These notifications initiate a security event review to detect any potential threats or suspicious activities. Depending on the outcome of the security threat assessment, users may regain access to their accounts. |

### 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

For publicly accessible systems:

Displays system use information [*Assignment: organization-defined conditions (FedRAMP Assignment: see additional Requirements and Guidance)*], before granting further access;

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

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: | |
| Parameter AC-8(a): | |
| Parameter AC-8(c)-1: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

**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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Req. 1** |  |
| **Req. 2** |  |
| **Req. 3** |  |

### 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: | |
| Parameter AC-10-1: | |
| Parameter AC-10-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-10 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter AC-11(a): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-11 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-11 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter AC-12: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-12 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter AC-14(a): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-14 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-17 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

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

The information system monitors and controls remote access methods.

| **AC-17 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-17 (1) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-17 (2) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter AC-17(3): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-17 (3) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter AC-17(4)(a): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-17 (4) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Parameter AC-17(9): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-17 (9) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-18 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Parameter AC-18 (1): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-18 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-19 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Parameter AC-19(5)-1: | |
| Parameter AC-19(5)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-19 (5) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-20 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-20 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Parameter AC-20(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-20 (2) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter AC-21(a): | |
| Parameter AC-21(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-21 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Parameter AC-22: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AC-22 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |

## Awareness and Training (AT)

### AT-1 Security Awareness and Training Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
2. A security awareness and training 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 awareness and training policy and associated security awareness and training controls; and
4. Reviews and updates the current:
5. Security awareness and training policy [*FedRAMP Assignment: at least every 3 years*]; and
6. Security awareness and training procedures [*FedRAMP Assignment: at least annually*].

| **AT-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter AT-1(a): | |
| Parameter AT-1(b)(1): | |
| Parameter AT-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **AT-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: CSO (Chief Security Officer) | |
| Parameter AT-2(c): Annually | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific   * Service Provider Hybrid (Corporate and System Specific)   ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AT-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | New employees to the company will be required to take security training since they will be dealing with sensitive and critical data. This security training consists of a mix of events: a team-specific security seminar (depends on what team an employee is at), a hands-on security assessment session (to correct employee security faults, if any), as well as a hands-on security training on our software platform(s) (this includes our own proprietary software as well as 3rd party software like AWS and database systems (depends on what team the employee is on). |
| **Part b** | If any information system were to change and it affects the security standards and/or policies of the company, all of the policies that used to be in place will be reviewed as well as will be instructed in a company-wide security seminar to announce and declare the new policies. This does not nullify the annual security assessment training done. Information system changes are changed whenever a vulnerability is discovered in our system that can be exploited. These changes are taken seriously and rewritten in much detail. |
| **Part c** | The awareness training is required to be completed annually for every onboarding of a new employee (which is team specific along with a general company-wide security training that applies to every incoming employee) as well as annually for everyone in the company. This security awareness training has many benefits to both the employee and the company; it provides training regarding spam, scam calls/emails/letters, proprietary software (i.e. Sentinel Shield), 3rd party software platforms (e.g. AWS), database systems (e.g. MySQL), as well as a talk on current events, vulnerable software and exploits that are currently being targeted at the time of training. This is done to have the employee gain awareness of the current issues and security threats happening around them that could also affect them and the company. |

#### 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: CSO (Chief Security Officer) | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific   * Service Provider Hybrid (Corporate and System Specific)   ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AT-2 (2) What is the solution and how is it implemented?** |
| --- |
| Besides doing general security training regarding our information systems, the security-related company-wide seminar also includes sections regarding recognizing insider threats. Employees working at Sentinel Shield will be taught to recognize when another employee (or person trying to disguise as an employee) is acting as an insider threat. Employees will be taught to log all of the evidence they gathered and report it to their corresponding manager or the CSO to be able to investigate and ultimately mitigate the threat. Insider threats will not be taken lightly. Any employee who is caught doing any type of action that is considered a threat to the company will be terminated immediately along with their access revoked and police called if it’s a major threat. If it’s just a minor threat, then they will still be terminated immediately, access revoked and blacklisted from the company. |

### 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: Program Manager / L1 Manager | |
| Parameter AT-3(c): | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AT-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | The trainee(New Employee) will be provided necessary training with respect to specific role, He/ She shall be made to go through lectures / classes to know the organization security policies and procedures. These trainings include various topics to understand the risks assosiated with the information systems, individual security responsibilitie and mititgations to make sure each individual understand information security and how to protect information systems and their data. |
| **Part b** | All the employees of the organization are required to do a training session whenever there is an change in the information system/ change in the role, the trainings are mandatory and if a individual is required to use the new information system, they shoudl clear the training in order to continue to use the information systems. The information systems include the operating systems, network infrastructures and licencesed applications. |
| **Part c** | After the initial training, all the individuals of the company are required to do these trainings annually to be up to date with the latest security policies. These trainings are made interactive to encourage the active learning to make sure everyone is aware of the security policies. |

#### AT-4 Security Training Records (L) (M)

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 one year*].

| **AT-4** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter AT-4(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AT-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

## Audit and Accountability (AU)

### AU-1 Audit and Accountability Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
2. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
4. Reviews and updates the current:
5. Audit and accountability policy [*FedRAMP Assignment: at every 3 years*]; and
6. Audit and accountability procedures [*FedRAMP Assignment: at least annually*].

| **AU-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter AU-1(a): | |
| Parameter AU-1(b)(1): | |
| Parameter AU-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **AU-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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*];

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;

Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

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: Security Officer | |
| Parameter AU-2(a): The system monitors and logs a variety of user activities and system events, including access attempts, administrative actions and data modifications inorder to ensure security and compliance. | |
| Parameter AU-2(d): Organization-defined subset of the auditable events that would be defined in AU-2 a and these should be audited continually for each identified event. | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | In the Software application, we can use the power of AWS CloudWatch tools to meticulously log and monitor critical system events to actively track and log both successful and unsuccessful account logon events, account management events, object access, policy changes, privileged functions, process tracking, and system events. Moreover, the web application has in-built functionalities to record all administrator activities, authentication checks, authorization checks, data deletions, data accesses and the data changes along with the permission changes. This setup not only encompasses tracking account logons, policy alterations, and system events, but also scrutinizes administrator activities and data modifications in web applications. Thus this robust system would facilitate seamless post-incident investigations, ensuring alignment with FedRAMP standards by creating a transparent and secure environment. |
| **Part b** | In the application we have established a collaborative framework where in our security team works closely with other departments in the organization to share important information about safety checks and audits. This coordination is facilitated through regular inter-departmental meetings and secure, integrated communication channels that enhance mutual support and assist in the careful selection of auditable events. Thus in this way, everyone helps each other to keep the system safe, meeting the strict rules set by FedRAMP. |
| **Part c** | We make sure that our auditing practices are robust and effective. Also, we clearly explain why we are auditing the specific events listed, primarily because these events hold critical information that can help us investigate any security incidents after they occur. Thus, by keeping a keen eye on these events, we can promptly identify and respond to any unusual activities, safeguarding the security of our system and protecting our organization from potential threats. This approach not only ensures our compliance with FedRAMP but also fortifies our defense mechanisms. |
| **Part d** | So we have picked a few specific events from the list in part A to watch closely all the time. We choose these events carefully because they are very important to keep our system safe. By always keeping an eye on these events, we can quickly spot and handle any security issues that might come up. This approach also follows FedRAMP's rules, showing that we are serious about maintaining high levels of security and following the rules. |

#### 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: Security Officer | |
| Parameter AU-2(3): Annual review and updates of audited events, aligned with changes in the threat environment as communicated by the JAB/AO. | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-2 (3) What is the solution and how is it implemented?** |
| --- |
| The organization maintains a dynamic approach to audit the critical events within the system. We ensure a comprehensive review and update of the audited events annually or whenever there's a significant alteration in the threat landscape as advised by the JAB/AO. This approach mainly allows us to up-to date of various potential vulnerabilities and to amend our audit strategies accordingly and also be prepared to handle any new risks that come up, keeping our system safe and sound. Our security team carefully handles the process, always staying alert and ready to adjust to changing threats, thereby safeguarding our organization's vital data assets and infrastructure. |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-3 What is the solution and how is it implemented?** |
| --- |
|  |

#### AU-3 (1) Control Enhancement (M)

The information system generates audit records containing the following additional information: [*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*]. The audit record types are approved and accepted by the JAB.

**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: | |
| Parameter AU-3(1): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-3 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: Information Security Officer | |
| Parameter AU-4: 256 GB Storage Space | |
| Implementation Status (check all that apply):  ✅ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-4 What is the solution and how is it implemented?** |
| --- |
| In accordance with the specific needs of our organization, we have established clear and detailed audit record storage requirement. We have established audit record retention timeframes that is 3 year, , after which we begin our clean-up. For our application, we use CloudTrail to record thorough audit logs and we regularly check storage capacity and set off proactive alerts when capacity reaches 200 GB so that we can take the necessary actions, like early cleanup or purchasing more storage as needed by the organization . Additionally, we only granted access to a selected group of user who has the necessary role to obtain audit records. System Administrator should be granted access to users according to their roles. |

### 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: System Administrator | |
| Parameter AU-5(a): Alerts the compliance team and stakeholders | |
| Parameter AU-5(b): Implement immediate mitigation measures, establish present and future monitoring procedures. | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | Identify the root causes of the audit processing failures. This includes examining the AWS configurations, security groups, IAM roles, and other relevant settings. The Compliance Team will be informed promptly about the audit processing failures, mitigation efforts, and any changes made to bring the system into compliance with the FedRAMP requirements. In addition, the Stakeholders and appropriate Administrators will be kept informed about the status and progress of these efforts to ensure transparency and accountability. |
| **Part b** | In response to the issues related to audit processing failures, we will promptly institute a series of corrective actions to mitigate the situation. These actions encompass several key steps. Firstly, we will make necessary adjustments to the AWS CloudWatch settings to ensure the proper collection and retention of logs, thus enhancing our monitoring capabilities. Additionally, we will update the IAM policies to provide the essential permissions required for efficient log access and analysis, streamlining our security protocols.  Furthermore, to bolster our security measures, we will introduce anomaly detection mechanisms designed to identify and promptly flag any unusual activities or behavior within our system. This proactive approach will aid in the early detection and response to potential threats.  Finally, we will conduct a comprehensive review of any third-party tools or services employed for log analysis. This review will ensure that these tools are not only effective but also fully compliant with established security standards, further strengthening our overall security posture. These measures collectively represent our commitment to addressing audit processing failures and enhancing the security of our systems.  All efforts undertaken to mitigate the audit processing failures will be meticulously documented. This documentation will encompass the recording of dates, specifics of alterations made, and the individuals accountable for implementing these modifications.  In addition to immediate actions, continuous monitoring procedures will be established to identify any potential recurrences of audit processing failures. This continuous oversight will be complemented by an ongoing review and enhancement of log management and audit processes to proactively prevent future issues.  Furthermore, to address any security incidents or breaches that may arise as a consequence of the audit processing failures, a comprehensive incident response plan will be in place. This plan includes defined communication and notification procedures to ensure a swift and coordinated response.  This approach ensures a systematic and accountable response to audit processing failures while maintaining adherence to compliance standards and promoting proactive security measures. |

### 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 [*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: | |
| Parameter AU-6(a)-1: | |
| Parameter AU-6(a)-2: | |
| Parameter AU-6(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: CSO (Chief Security Officer) in conjunction with the COO (Chief Operations Officer) | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-6 (1) What is the solution and how is it implemented?** |
| --- |
| Security assessments along with company-wide operations regarding analysis and investigation is part of both the CSO’s and the COO’s job. Creating these workflows is a very important part of the company. It allows the company to flexibly and meticulously log all of the past and current investigations happening at the company. In regards to audit reviews, this is done by both the CSO and the COO, since it’s a full company-wide audit which includes internal security and company-wide operations. The COO will be in charge of putting the plan in-place and the CSO will then complete the analysis needed to have a successful audit. In regards to security threats and suspicious activity, the CSO will be in full charge of this area since they’re in charge of managing, logging and analyzing any type of security threat that occurs at the company. |

#### 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: CSO / Information Auditor | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-6 (3) What is the solution and how is it implemented?** |
| --- |
| The organization has an internal auditing tool, which correlates all the incidents and informtion required for the auditor. The custom tool has predefined rules to correlate the information and identify the incidents, All these incidents will be monitored by the Information auditors and security officers if required. All the actions related to the incidents shall be reviewed by the CSO and necessary action is to be taken. Based on the volume and priority of the information and incidents the respective members shall be tagged to each incident to work on. |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-7 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Parameter AU-7(1): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-7 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter AU-8(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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) 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)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter AU-8(1)(a)-1: | |
| Parameter AU-8(1)(a)-2: | |
| Parameter AU-8(1)(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-8 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-9 What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter AU-9(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-9 (2) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter AU-9(4): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-9 (4) What is the solution and how is it implemented?** |
| --- |
|  |

### AU-11 Audit Record Retention (M)

The organization retains audit records for [*FedRAMP Assignment: at least ninety (90) days*] 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: | |
| Parameter AU-11: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-11 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter AU-12(a): | |
| Parameter AU-12(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **AU-12 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

## Security Assessment and Authorization (CA)

### CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
2. Reviews and updates the current:
   1. Security assessment and authorization policy [*FedRAMP Assignment: at least every three (3) years*]; and
   2. Security assessment and authorization procedures [*FedRAMP Assignment: at least annually*].

| **CA-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter CA-1(a): | |
| Parameter CA-1(b)(1): | |
| Parameter CA-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **CA-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
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: CSO (Chief Security Officer) | |
| Parameter CA-2(b): Annually | |
| Parameter CA-2(d): COO (Chief Operations Officer) and IT/Software Engineering Manager | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. Date of Authorization, | |

| **CA-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | The Security Assessment plan has been implemented by our CSO (Chief Security Officer). The Security Assessment plan covers everything related to security controls and procedures at Sentinel Shield. The Security Assessment plan is implemented in collaboration with the COO (Chief Operations Officer) and IT and Software Engineering managers. The COO is in charge of making sure that the Security Assessment plan applies well to everyone in the company (administration, business operations, HR, Product Operations, etc). The IT and Software Engineering managers are in charge of applying the policies to their own sub-teams and making sure that it’s as stable as can be. The CSO then finalizes the policies and re-checks with the collaboration team. |
| **Part b** | The Security Assessment is reassessed and implemented annually. The CSO acknowledges that every year technology changes drastically to some degree. The Security Assessment is, has to be and will be reassessed annually to ensure that security standards are heavily up to date with current real-world standards. |
| **Part c** | The Security Assessment document follows the Security Assessment plan, which implements the policies and procedures of the Security Assessment plan. This document has been written by our CSO (Chief Security Officer) using Microsoft Word. Our Microsoft account is tightly secured using Two-Factor Authentication along with role-based access in Microsoft Word Online documents. Since the document is being collaborated on, only the people with specific access are able to access the document. |
| **Part d** | The finalized Security Assessment document is re-evaluated by the CSO (Chief Security Officer), COO (Chief Operations Officer) and the IT & Software Engineering managers. Once finalized by everyone in the collaborating team, the plan is then presented to AWS (our 3rd party assessor) who will be in charge of executing the completed plan. They will also have the authority to execute or add any other necessary steps to the plan. |

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

The organization employs assessors or assessment teams with [*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: Sentinel Shield In-House Security Team | |
| Parameter CA-2(1): Low Level of Independence | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-2 (1) What is the solution and how is it implemented?** |
| --- |
| Amazon Web Services (AWS), who is FEDRAMP qualified for conducting security assessments, is in charge of executing the organization-wide security assessment. The reason it’s AWS is because our internal systems are already AWS so it makes it even easier for them to get to know our architecture. The sub-team leads for each department are also in charge of enforcing the security assessment policies, but the AWS assessment team is mainly in charge of executing the plan in-place. Since Sentinel Shield is a company that holds a lot of customer critical data that cannot be leaked. AWS is in charge of keeping the policies assessed and enforced. AWS has the authority to execute every step necessary to have a successful security assessment (e.g., monitoring, employee questioning, database analysis, network analysis, etc). |

#### 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; insider threat assessment; performance/load testing;* [*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: CSO (Chief Security Officer) | |
| Parameter CA-2(2)-1: Annually | |
| Parameter CA-2(2)-2: Internally Announced | |
| Parameter CA-2(2)-3: In-Depth Monitoring, Service Vulnerability Scanning, Malc. User Testing, Insider and Outsider Threat Assessment, Performance/Load Testing of servers, Server Vulnerability Scanning and Assessment, Database Vulnerability Scanning | |
| Parameter CA-2(2)-4: Other forms of Security Assessment include: random interviews with people at the company to assess their security standards and assess if they’re an intentional (or unintentional) insider threat as well as have interviews with Database Administrators and System Administrators about how they maintain security standards for the company-related systems | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-2 (2) What is the solution and how is it implemented?** |
| --- |
| The CSO (Chief Security Officer) is in charge of annually leading the Security Assessment plan and execution with the help of our 3rd party assessment team (AWS). The assessment is internally announced, it is not announced to the public due to security reasons. The Security Assessment includes assessments like: In-depth monitoring, service vulnerability scanning, malicious user testing, Insider and outsider threat assessment, performance & load testing of servers, server vulnerability scanning and assessment and database vulnerability scanning. Our in-depth monitoring system consists of scanning through all of the available machines at Sentinel Shield.  To primarily identify all of the machines, we use FileWave, an MDM software that is installed on every machine at the company to be able to track and manage each machine. Since every machine will be on the company subnet(s), the assessment team will be able to see all of the installed software on all of the machines and create a report about it. If there’s any software that’s unauthorized for any reason, FileWave is able to flag it and an assessor is able to remove the software immediately. Service vulnerability scanning is also considered to be part of this process as FileWave is able to identify all of the machines and unverified software. The assessment team is also able to use tools like nmap to do more in-depth analysis on certain (or all) machines on our system to scan for vulnerabilities in any machine, server and database. |

#### 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: | |
| Parameter CA-2(3)-1: Sentinel Shield’s internal systems | |
| Parameter CA-2(3)-2: AWS (Amazon Web Services) – FEDRAMP Qualified | |
| Parameter CA-2(3)-3: Policies and security policies said in completed Security Assessment Plan and approved by assessor (AWS). | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-2 (3) What is the solution and how is it implemented?** |
| --- |
| Once the Security Assessment is completed, AWS will return to us with the results, either with an approval or denial of our (intended) security policies and what to improve on. If denied or found many errors in our policies, our CSO (Chief Security Officer) along with the COO (Chief Operations Officer) will need to assemble another plan improving on the details given by AWS. If approved, then the policies will be heavily enforced by the CSO, and the department leads of each department at the company. |

### 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 CSP Name System Connects To** | **Role and Name of Person Who Signed Connection Agreement** | **Name and Date of Interconnection Agreement** |
| --- | --- | --- | --- |
| Sentinel Shield Software 1.0 | Agency 134564  (AWS Lambda & AWS WAF) | John Matt,Chief Information Security Officer | January 10, 2023 |
| Sentinel Shield Data Storage | Agency 156723  (AWS S3 & AWS Glacier) | Jane Smith, Chief Data Officer | March 12, 2023 |
| Sentinal Shield Analytics xSystem | Agency 194562  (AWS Analytics & AWS Redshift) | Randy Lee, Chief Technology Officer | May 19, 2023 |
| Sentinel Shield Communications Systems | Agency 145334  ( AWS SNS) | Luke Davis, Chief Communications Officer | June 20, 2023 |

| **CA-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System owner | |
| Parameter CA-3(c): | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | The system owner authorizes the connections for the information systems in the organization, these security agreements are made for each individual applization or service. The responsible POC for each applicaiton and an external POC for the will be included in the agreement to make sure each application or service is according to ot the security guidelines of the company. All the security agreements are made through physical medium and all the outgoing / incoming services data will be monitored through the AWS cloudtrail. cloudTrail monitors all the API calls being made from each service and helps to investigate the security incidents. |
| **Part b** | All the connections made from the applications / services or interconnections made from the individual teams within the company are documented by the system owner and maintained on bi-annually basis and review will be conducted when required or there is an update on the applications / services. The documentation includes the architecture diagrams and conncections between different components as it serves as blueprint for all the services being consumed or pulling data from other services. |
| **Part c** | All the agreements made are documented properly and they will be reviewed the system owners internally on monthly basis, The responsible vice-president will go through the security documents on annual basis to make sure all are on same page. Changes would be suggested and made on the annual meetings. All the connections to third party services and interconnectivity between different services will be reviewed based on usage and need, therefore if required unused connections would be terminated. |

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

The organization prohibits the direct connection of an [*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: Security Manager | |
| Parameter CA-3(3)-1: Implementation of boundary protections according to TIC requirements. | |
| Parameter CA-3(3)-2: Prohibition of direct connections from defined unclassified, non-national security systems to external networks. | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-3 (3) What is the solution and how is it implemented?** |
| --- |
| Our system security is fortified using the best possible AWS robust infrastructure under the supervision of the Security Manager. This framework prevents unclassified, non-national security systems from directly connecting to external networks without adhering to Trusted Internet Connection (TIC) regulations. We utilize AWS Lambda for serverless computing, enhancing efficiency and resource optimization. Alongside this, we have also deployed AWS WAF i.e Web Application Firewall and Shield, establishing a resilient firewall that actively deters potential security threats.Moreove, in our setup we also integrated the AWS VPC to create a secure and isolated segment within the AWS Cloud, giving us full control over our virtual networking environment. This environment is meticulously configured to maintain a strong security, while AWS IAM manages access to resources securely, allowing granular control over application security. Complementing this is AWS CloudTrail, which facilitates easy compliance tracking and enables quick response to any system irregularities, ensuring the resilience and security of our application. |

#### CA-3 (5) Control Enhancement (M)

The organization employs [*Selection: allow-all, deny-by-exception, deny-all, permit by exception*] policy for allowing [*Assignment: organization-defined information 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: Cloud Security Manager | |
| Parameter CA-3(5)-1: Policy Choice: "deny-by-exception". | |
| Parameter CA-3(5)-2: External Information Systems: Public cloud services, third-party APIs. | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate   * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-3 (5) What is the solution and how is it implemented?** |
| --- |
| In the AWS-hosted application, we employ a deny-by-exception policy, which restricts connections to external systems except for necessary, predefined systems based on operational requirements. The core of our security strategy is the AWS WAF which is a web application firewall that scrutinizes traffic and blocks potential threats, coupled with AWS Identity and Access Management (IAM) which governs role-based access controls. This creates a strong first line of defence which also aligns with FedRAMP's high standards. Moreover inorder to bolster security, we utilize AWS Lambda to automate security workflows and enable rapid response to potential issues. Mainly we use AWS CloudTrail and AWS CloudWatch tools aid in continuous monitoring, providing insights and activity logs within our environment. This, along with secure protocols for interactions with third-party vendors, forms a robust security infrastructure. It showcases our dedication to safeguarding our data assets, upholding a secure and trustworthy working environment. |

### 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/](https://www.fedramp.gov/resources/documents)

| **CA-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter CA-5(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Parameter CA-6(c): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

### 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

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

| **CA-7** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter CA-7(a): | |
| Parameter CA-7(b)-1: | |
| Parameter CA-7(b)-2: | |
| Parameter CA-7(g)-1: | |
| Parameter CA-7(g)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-7 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |
| **Part f** |  |
| **Part g** |  |

**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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-7 What is the solution and how is it implemented?** | |
| --- | --- |
| **Req. 1** |  |
| **Req. 2** |  |
| **Req. 3** |  |

#### 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: | |
| Parameter CA-7(1): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-7 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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

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

| **CA-8** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter CA-8-1: | |
| Parameter CA-8-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-8 What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-8 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter CA-9(a): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CA-9 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

## Configuration Management (CM)

### CM-1 Configuration Management Policies and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]:*
2. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
4. Reviews and updates the current:
5. Configuration management policy [*FedRAMP Assignment: at least every three (3) years*]; and
6. Configuration management procedures [*FedRAMP Assignment: at least annually*].

| **CM-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter CM-1(a): | |
| Parameter CM-1(b)(1): | |
| Parameter CM-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **CM-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: Chief Information Security Officer (CISO) | |
| Implementation Status (check all that apply):  ✅ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-2 What is the solution and how is it implemented?** |
| --- |
| Within our application, we have a structured approach to identify and document all the configuration items present in our AWS environment . Each CI whether it is a database instance, or a network component, is carefully cataloged and marked for easy identification. ​​If there are any requests to modify the default configuration, the Chief Information Security Officer ensures that they are properly recorded, examined, and approved in accordance with established protocol. We have maintained comprehensive records that included version tracking, changes histories to ensure a complete understanding of the system's configuration. We are using an AWSCloudwatch alarm to monitor that the ​​ deployed configuration complies with the agreed baseline, and we immediately resolve any unauthorized changes or deviations to maintain security and compliance. |

#### CM-2 (1) Control Enhancement (M)

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

1. [*FedRAMP Assignment: at least annually*];
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)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter CM-2(1)(a): | |
| Parameter CM-2(1)(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-2 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

#### 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: Configuration Management Specialist | |
| Implementation Status (check all that apply):  ✅ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-2 (2) What is the solution and how is it implemented?** |
| --- |
| We have developed a strong automated infrastructure to ensure that our application always has a complete, accurate, and easily available baseline configuration. We are using AWS CloudFormation for our application for code deployment and AWS Systems Manager for automated operations like patch management and compliance assessment. Also, we are utilizing AWS Config to continuously monitor AWS resources and record configuration changes. To proactively identify any deviations from our baseline configuration, we make use of AWS CloudWatch alarms. In our organization, Configuration management specialist is responsible for monitoring these mechanisms and defining and enforcing policies. AWS administrators conduct routine audits of configuration records to confirm their accuracy and completeness. Also, our staff receives regular training and updates to ensure that they are knowledgeable on AWS services and best practices |

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

The organization retains [*Assignment: organization-defined previous versions of baseline configurations of the information system*] to support rollback.

| **CM-2 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: AWS Administrator | |
| Parameter CM-2(3): Retains previous versions of baseline configurations of the system to support rollback. | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-2 (3) What is the solution and how is it implemented?** |
| --- |
| ​​Configuration management within AWS is accomplished through a combination of AWS Config, AWS CloudFormation, and AWS Systems Manager. AWS Config is configured to continuously track changes in resource configurations, including AWS resource relationships and changes over time. We employ AWS CloudFormation for infrastructure provisioning and configuration management, utilizing version control for templates. AWS Systems Manager Automation documents are used for configuration automation, patch management, and version control. In the event of an issue or security incident, the system owner or designated personnel initiate a rollback request. AWS CloudFormation templates for previous known good configurations are identified. Templates are deployed using AWS Systems Manager Automation to revert the environment to the specified baseline. Rollback procedures are regularly tested in non-production environments to ensure their effectiveness. Records of previous baseline configurations are maintained through AWS Config, which captures historical configuration states and changes. Screenshots of AWS Config history and relevant logs are stored for auditing purposes. |

#### 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: Services Administrator | |
| Parameter CM-2(7)(a)-1: devices preconfigured to mitigate risks associated with the destination | |
| Parameter CM-2(7)(a)-2: pre configured software to mitigate risks | |
| Parameter CM-2(7)(b): Apply security safeguards | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-2 (7) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | The organization identifies specific information systems, system components, or devices and assigns configurations tailored to the security requirements of individuals traveling to significant-risk locations. Before departing for these locations, travelers are provided with devices preconfigured to mitigate risks associated with the destination, including cybersecurity threats. This process ensures that individuals have the necessary safeguards in place to enhance security during their travel. Records are maintained documenting the issuance of devices with specific configurations to traveling individuals and the subsequent application of security safeguards upon their return. An audit trail is established to track the status and history of devices issued to travelers, including any security incidents or deviations from standard configurations. |
| **Part b** | After individuals return from significant-risk locations, security safeguards are applied to their devices. These safeguards encompass comprehensive security checks, including malware scans and the verification of baseline configurations to ensure alignment with standard, secure settings. Any deviations or security concerns are promptly addressed to restore the devices to a secure state, mitigating potential risks before they can impact the system's integrity. |

### 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: | |
| Parameter CM-3(e): | |
| Parameter CM-3(g)-1: | |
| Parameter CM-3(g)-2: | |
| Parameter CM-3(g)-3: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |
| **Part f** |  |
| **Part g** |  |

### 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: System Administrator | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-4 What is the solution and how is it implemented?** |
| --- |
| Before any changes are introduced, a thorough pre-change analysis is carried out. This analysis encompasses the identification of proposed changes, their scope, and the intended purpose. Furthermore, it involves an assessment of the potential security implications these changes may have, such as vulnerabilities, risks, and potential non-compliance issues. The goal is to gain a clear understanding of how these changes could affect the confidentiality, integrity, and availability of the system's data and resources. Our approach to security impact assessment involves a systematic analysis of the potential consequences associated with each proposed change. Risks linked to these changes are identified and evaluated based on their potential impact and likelihood. Detailed documentation of this assessment is maintained, encompassing findings, risk assessments, and suggested mitigations to address any identified security concerns. The approval or disapproval of changes hinges on the outcomes of the security impact assessment. In cases where security impacts are identified, implementation of mitigation measures designed to diminish or eliminate associated risks are done. These mitigation measures are meticulously documented and their effectiveness verified. Approved changes are executed in strict adherence to established procedures and security guidelines. Following implementation, these changes are subjected to ongoing monitoring to ensure that anticipated security impacts are being effectively managed. Continuous monitoring allows us to promptly address any unexpected security vulnerabilities or issues that may arise post-change 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-5 What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-5 (1) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter CM-5(3): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-5 (3) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter CM-5(5)(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-5 (5) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Parameter CM-6(a)-1: | |
| Parameter CM-6(a)-2: | |
| Parameter CM-6(c)-1: | |
| Parameter CM-6(c)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |

#### 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: | |
| Parameter CM-6(1): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-6 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter CM-7(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. Date of Authorization, | |

| **CM-7 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Parameter CM-7(1)(a): | |
| Parameter CM-7(1)(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-7 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Parameter CM-7(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-7 (2) What is the solution and how is it implemented?** |
| --- |
|  |

#### CM-7 (5) Control Enhancement (M)

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 annually or when there is a change*].

| **CM-7 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter CM-7(5)(a): | |
| Parameter CM-7(5)(c): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-7 (5) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

### CM-8 Information System Component Inventory (L) (M) (H)

The organization:

1. Develops and documents an inventory of information system components that:
2. Accurately reflects the current information system;
3. Includes all components within the authorization boundary of the information system;
4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and
6. 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: | |
| Parameter CM-8(a)(4): | |
| Parameter CM-8(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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.

*Instruction: A description of the inventory information is documented in Section 10. It is not necessary to re-document it here.*

*Delete this and all other instructions from your final version of this document.*

| **CM-8 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-8 (1) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter CM-8(3)(a): | |
| Parameter CM-8(3)(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-8 (3) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-8 (5) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-9 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-10 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

#### 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: | |
| Parameter CM-10(1): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-10 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter CM-11(a): | |
| Parameter CM-11(b): | |
| Parameter CM-11(c): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CM-11 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

## Contingency Planning (CP)

### CP-1 Contingency Planning Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
2. A contingency 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 contingency planning policy and associated contingency planning controls; and
4. Reviews and updates the current:
5. Contingency planning policy [*FedRAMP Assignment: at least every three (3) years*].; and
6. Contingency planning procedures [*FedRAMP Assignment: at least annually*].

| **CP-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter CP-1(a): | |
| Parameter CP-1(b)(1): | |
| Parameter CP-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **CP-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### CP-2 Contingency Plan (L) (M) (H)

The organization:

1. Develops a contingency plan for the information system that:
2. Identifies essential missions and business functions and associated contingency requirements;
3. Provides recovery objectives, restoration priorities, and metrics;
4. Addresses contingency roles, responsibilities, assigned individuals with contact information;
5. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
6. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
7. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];
8. Distributes copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];
9. Coordinates contingency planning activities with incident handling activities;
10. Reviews the contingency plan for the information system [*FedRAMP Assignment: at least annually*];
11. 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;
12. Communicates contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*]; and
13. 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: Chief Security Officer (CSO) | |
| Parameter CP-2(a)(6): Review Contingency plan document | |
| Parameter CP-2(b): Identify individual who need access to the contingency plan | |
| Parameter CP-2(d): CSO officer handles the communication between planning and incident handling activities. | |
| Parameter CP-2(f): Check for what changes are required to the contingency plan | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | We have developed a contingency plan for the information system. We have carefully identified the important processes and operations that rely on our AWS configuration and decide what we should do in case something goes wrong. We set timelines for when we should get things back on track, ranking which components should be repaired first. We make sure we have data backups to support our services during outages. Crucially, we've established roles and responsibilities, with designated team members and contact information. This extends to technical teams responsible for system recovery. We use effective tactics like disaster recovery plans and automated failover mechanisms supplied by AWS services to protect our operations even in the face of system problems. Identity and Access Management (IAM) keeps security in place. Importantly, our contingency plan is reviewed every quarter and approved by persons or positions established by our business, assuring alignment with its objectives and needs. |
| **Part b** | We have identified essential divisions and key employees, like security specialists, system administrators, and emergency response teams. We then supply them with our contingency plan which outlines specific actions to take in response to system problems and to resume operations. We combine physical and digital versions of the contingency plan to implement this distribution successfully, enabling access under any conditions. Having copies of the plan on hand allows the responsible department to rapidly start corrective action in the event of a security incident |
| **Part c** | For the maintenance of business operations, our organization has implemented seamless cooperation between incident handling and contingency planning. Together with the incident handling team, a group with the necessary technical knowledge to successfully carry out these contingency plans, we execute our contingency plan. Even If there is any kind of issue, this coordinated approach ensures the smooth running of business operations. |
| **Part d** | The company has contingency plans for each team and a team member is taken part of the review process every year who is familiar with all the systems. These annual reviews would be done in the presence of division VP and required persons. Any update required updates to the plan should be made to the plan and will be communicated to all the relevant personnel. |
| **Part e** | The company may be required to update their contingency plan when there are changes in the company's structure or any technical infrastructure. Sometimes new laws in the country may also lead to updating the company contingency plan. Along with the updates some contingency plans may be difficult to implement and some may have problems in the execution, during these times necessary changes are to be made on the spot with approval from the VP and communicate the respective required personnel. |
| **Part f** | The company requires communicate the contingency plan changes or updates to all the respective required personnel on a safe channel. This is to make sure that the contingency plan prevents unauthorized disclosure or modification. All the data related to the contingency plan would be saved on cloud with limited access with encryption. |
| **Part g** | We have taken a number of precautions to protect our contingency plan from unwanted access and modifications. We safeguard it with powerful locks and security methods like secret codes. Only the intended viewers can see it and we keep track of who does so. We have educated employees about the importance of safeguarding the plan. Additionally, to ensure that nobody can access the system or alter the plan without authorization, we routinely review and enhance our security. |

#### 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: Chief Security Officer (CSO) | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-2 (1) What is the solution and how is it implemented?** |
| --- |
| The Chief Security Officer (CSO) is responsible for leading, designing and coordinating the contingency plan in the case of a cybersecurity threat. The development of the contingency plan is led by the CSO, the plan consists of meeting with the Chief Operations Officer (COO) to be able to create a viable and successful plan for any type of insider and/or outsider threat. The development of the contingency plan consists of several meetings discussing the pre-requisites, procedures and policies of said contingency plan. These meetings are done over a period of the first quarter (Q1) of the year (it is completed annually). These meetings take place every Friday of the week until the review is completed. If any changes arise during the development of the plan (e.g, a new policy regarding insider threats needs to be added), they will be carefully reviewed by the CSO and the COO so that it can be added to the contingency plan as soon as possible. |

#### 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: Chief Security Officer (CSO) and COO (Chief Operations Officer) | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-2 (2) What is the solution and how is it implemented?** |
| --- |
| The CSO (Chief Security Officer) and the COO (Chief Operations Officer) are both in charge of capacity planning for the organization’s contingency operations. The COO is in charge of determining the needs of the entire organization regarding the contingency plan and the CSO is in charge of implementing such needs so that the contingency plan can be developed and executed at its highest potential with all of its needs successfully met. Regarding information processing and environmental support, the needs consist of making sure that all internal and critical customer data is intact (and if not, then the CSO follows ahead with the policy regarding stolen data and proceeds to contact the affected customer) in the case of any active or possible threat. Regarding telecommunication, if there’s an active and/or possible threat, then internal communication is key (according to the plan itself) and external services will be turned off so data cannot be leaked or threatened. |

#### 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: Chief Security Officer (CSO) and COO (Chief Operations Officer) | |
| Parameter CP-2(3): Between 24 to 72 hours or ASAP if resolved | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-2 (3) What is the solution and how is it implemented?** |
| --- |
| Since our services are crucial to our customers, the contingency plan states to be back in service between 24 to 72 hours or as soon as possible. Since our service is an emergency and reporting service, it is crucial that our customers get back the service as soon as Sentinel Shield resolves their issue. The Chief Security Officer (CSO) and the Chief Operations Officer (COO) are in charge of organizing and resolving the organization operations during a threat (this falls under the contingency plan). If an active threat is resolved (or a possible threat is resolved to be untrue), then services will be back online immediately. If an active threat is not resolved, then the affected customers will be communicated with immediately. This conversation with the customer will have a description of the current threat as well as the mitigation techniques to assure that their data will be safe (if data is indeed compromised, it will be communicated as well; this falls under the contingency plan as well). |

#### 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: CSO , Systems security officer | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-2 (8) What is the solution and how is it implemented?** |
| --- |
| The idea is to develop a contingency plan for organization information. The company backs up the data using the AWS cloud solutions like S3 for documents and glacier for objects for long term backup and EBS is used to save instance data and amazon backup to save the data related to working projects. On premise backup solutions like physical hard disks are also used to save the sensitive data on physical devices by the respective VP’s and employees. The company also has on premise backup servers in offices to save data on the go which are essential for certain functions of the company. |

### 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: | |
| Parameter CP-3(a): | |
| Parameter CP-3(c): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-3 What is the solution and how is it implemented?** |
| --- |
|  |

### CP-4 Contingency Plan Testing (M)

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: | |
| Parameter CP-4(a)-1: | |
| Parameter CP-4(a)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-4 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-6 (1) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-6 (3) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter CP-7(a)-1: | |
| Parameter CP-7(a)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-7 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-7 (1) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-7 (2) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-7 (3) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter CP-8-1: | |
| Parameter CP-8-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-8 What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-8 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-8 (2) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter CP-9(a): | |
| Parameter CP-9(b): | |
| Parameter CP-9(c): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-9 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |

#### CP-9 (1) Control Enhancement (M)

The organization tests backup information [*FedRAMP Assignment: at least annually*] to verify media reliability and information integrity.

| **CP-9 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter CP-9 (1): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-9 (1) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter CP-9(3): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-9 (3) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-10 What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **CP-10 (2) What is the solution and how is it implemented?** |
| --- |
|  |

## Identification and Authentication (IA)

### IA-1 Identification and Authentication Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
2. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
4. Reviews and updates the current:
5. Identification and authentication policy [*FedRAMP Assignment: at least every three (3) years*]; and
6. Identification and authentication procedures [*FedRAMP Assignment: at least annually*].

| **IA-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter IA-1(a): | |
| Parameter IA-1(a): | |
| Parameter IA-1(b)(1): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **IA-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: Security Officer | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate   * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-2 What is the solution and how is it implemented?** |
| --- |
| The deployment of Amazon Cognito is pivotal for ensuring unique identification and robust authentication of organizational users within the AWS ecosystem. It seamlessly integrates with AWS's Identity and Access Management (IAM), providing streamlined and secure control over user permissions and roles. This structure allows for comprehensive monitoring and management, ensuring each user or process is distinctively identified and authenticated. Relating to the network structure, Amazon Cognito collaborates effectively with Amazon API Gateway and AWS Lambda in our AWS-based setup. The API Gateway, connected to Lambda functions, ensures secure, automated, and efficient authentication processes. This integration within the network diagram emphasizes the clear, secure path from user login to the assignment of appropriate permissions, upholding the high-security standards. |

#### 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: Network Administrator | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate   * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-2 (1) What is the solution and how is it implemented?** |
| --- |
| We use AWS Multi-Factor Authentication (MFA), an essential component in providing additional security by requiring two or more separate forms of identification. The Network Administrator ensures the enforcement of MFA for network access to privileged accounts. Implementation involves configuring AWS MFA for all privileged accounts within the system. Users must provide not just a username and password, but also a unique authentication code from their AWS MFA device, thus ensuring an additional layer of security. Regular audits and reviews are conducted to ensure the effectiveness and compliance of the MFA system with FedRAMP standards. Proper documentation is maintained to keep track of the MFA settings and configurations, ensuring a secure and robust authentication mechanism for privileged network access. |

#### 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: Security Administrator | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)   * Configured by Customer (Customer System Specific)   ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-2 (2) What is the solution and how is it implemented?** |
| --- |
| We implemented multi factor authentication (MFA) for all network access to non-privileged accounts. The chosen technology for this purpose is AWS Multi-Factor Authentication (MFA), a simple best practice that adds an extra layer of protection on top of the username and password. It leverages various MFA devices to ensure the identity of the users and limit the access only to those who pass the multifactor authentication process. AWS MFA integrates with AWS services and directory service products, requiring users to provide unique authentication from their MFA device to access the AWS Management Console, AWS CLI, and AWS API operations. By employing AWS MFA, the organization ensures enhanced security by requiring two or more separate forms of identification during the login process. This additional security layer helps protect non-privileged accounts, thereby aligning the organization with FedRAMP's heightened security standards and regulations. |

#### 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: Security Administrator | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate   * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-2 (3) What is the solution and how is it implemented?** |
| --- |
| We deployed a robust solution for ensuring the security of local access to privileged accounts through the implementation of multifactor authentication (MFA). This system is realized through the integration of Amazon Web Services (AWS) MFA, enhancing security by necessitating two or more distinct forms of identification for local access. Beyond the usual username and password, users must validate their identities using a secure and approved MFA device. The setup process involves configuring the AWS MFA to function seamlessly with the organization’s local servers and systems. Users attempting to gain local access to privileged accounts are prompted to provide additional authentication information from their MFA device. This could be a time-sensitive token or a push notification approval via a smartphone app. Utilizing AWS’s robust and secure infrastructure, this MFA setup ensures that local access to privileged accounts is meticulously monitored and controlled, adding a significant layer of security and ensuring compliance with FedRAMP standards. |

#### 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: IAM Administrator | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-2 (5) What is the solution and how is it implemented?** |
| --- |
| A comprehensive and sophisticated authentication mechanism has been meticulously established to adhere to the requirements needed. This mechanism is meticulously designed to ensure that even when group authenticators are employed to facilitate specific functionalities or access levels, individual users are unequivocally mandated to authenticate themselves using their unique authenticators. This control enhancement leverages cutting-edge authentication technologies and best practices. It entails the implementation of robust identity and access management (IAM) systems, which are integral to enforcing individual authentication within the context of group authentication.  In practical terms, pivotal technologies such as Single Sign-On (SSO) and multi-factor authentication (MFA) play crucial roles. SSO simplifies user access by enabling them to authenticate once, while MFA adds an additional layer of security by requiring multiple authentication factors. Furthermore, the system incorporates the use of access control lists (ACLs) and role-based access control (RBAC) mechanisms. These technologies provide fine-grained control over user permissions and access, ensuring that individual authentication remains uncompromised, even in scenarios where group authenticators are utilized.  In conclusion, the organization has implemented an advanced authentication mechanism. It harnesses state-of-the-art authentication technologies such as SSO, MFA, ACLs, and RBAC, ensuring that individual users must authenticate themselves with their unique authenticators, even within a group authentication context. This robust authentication approach enhances security, individual accountability, and access control, thereby fortifying the overall security posture of the system. |

#### 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: IAM Administrator | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-2 (8) What is the solution and how is it implemented?** |
| --- |
| Replay-Resistant Authentication Mechanisms are a vital component ensuring the security of network access to privileged accounts. These mechanisms encompass Multi-Factor Authentication (MFA), which obliges all privileged accounts to employ MFA, combining something known to the user (e.g., a password) with something possessed (e.g., a mobile device token). Additionally, Time-Based Authentication Tokens are employed, creating time-sensitive tokens that expire quickly, rendering replay attacks impractical. Furthermore, robust Session Encryption, implemented through encryption protocols like TLS, is in place to thwart eavesdropping and unauthorized access.  Regarding implementation, MFA enforcement is achieved through AWS Identity and Access Management (IAM) policies, tightly integrated with AWS MFA services. Time-based tokens are generated using industry-standard time-based one-time password (TOTP) algorithms. Additionally, session encryption is ensured through AWS Security Groups and Network Access Control Lists (ACLs), which facilitate secure communication between clients and AWS services.  Continuous monitoring is essential to ensure the effectiveness of these replay-resistant mechanisms. This monitoring is conducted through AWS CloudWatch logs and security alerts. Regular reviews and audits of authentication logs are also carried out to promptly identify and respond to any irregularities or suspicious activities. Furthermore, mechanisms are diligently updated with the latest security patches and configurations to proactively address emerging threats.  In the unfortunate event of a security incident related to network access involving privileged accounts, an established incident response protocol comes into play. This includes the immediate isolation of affected accounts, in-depth analysis of logs and incident forensics to determine the scope and impact of the breach, prompt notification of relevant authorities and stakeholders, and the implementation of remedial measures aimed at preventing future incidents. |

#### 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: IAM Administrator | |
| Parameter IA-2(11): FIPS 140-2 | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-2 (11) What is the solution and how is it implemented?** |
| --- |
| Implemented a robust multi factor authentication (MFA) framework to bolster the security of remote access, encompassing both privileged and non-privileged accounts. Under this MFA scheme, individuals seeking access are required to provide a minimum of two distinct authentication factors. This stringent approach fortifies the overall security of the system, ensuring that access is tightly controlled and safeguarded.  A pivotal aspect of this control revolves around the demand that one of the authentication factors originates from a device that rigorously adheres to recognized and stringent security standards. Either of the three standard that must be included are:   1. **FIPS 140-2:** This standard mandates a thorough validation process for the cryptographic modules within the device, overseen by the Cryptographic Module Validation Program (CMVP). Moreover, these modules must strictly align with the Federal Information Processing Standards (FIPS) 140-2, attesting to their robust security features. 2. **NIAP Certification:** The device must obtain certification from the National Information Assurance Partnership (NIAP), signifying its adherence to rigorous security standards. This certification ensures that the device meets the stringent criteria essential for safeguarding sensitive access. 3. **NSA Approval:** Additionally, the device must receive explicit approval from the National Security Agency (NSA). This endorsement confirms the device's suitability for enhancing the security of remote access while aligning seamlessly with the NSA's exacting security standards.   A robust multi factor authentication mechanism is implemented for remote access to both privileged and non-privileged accounts. This authentication method mandates the use of at least two distinct factors for verification, with one of these factors originating from a device that is independent of the system seeking access. The particular device chosen must meet the stringent criteria outlined as follows FIPS 140-2. It is of paramount importance to thoroughly review and tailor this provided information to ensure its precise alignment with the requisite security standards.  Furthermore, there are supplementary FedRAMP requirements and guidance to reinforce the multifactor authentication (MFA) strategy, including the use of Personal Identity Verification (PIV) credentials. Of particular note is the stipulation that one of the authentication factors must be provided by a separate device. By mandating that one of the authentication factors originates from a device compliant with specific security standards, this control significantly elevates the overall security posture of the system. It ensures that remote access to both privileged and non-privileged accounts is fortified, rigorously controlled, and effectively safeguarded against unauthorized intrusion. |

#### 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: IAM Administrator | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-2 (12) What is the solution and how is it implemented?** |
| --- |
| Within the system, a sophisticated framework is in place for the acceptance and electronic verification of Personal Identity Verification (PIV) credentials. This framework goes a step further by extending its capabilities to include the validation of Common Access Card (CAC) credentials, representing the Department of Defense's (DoD) specific implementation of PIV, meticulously adhering to Federal Information Processing Standards (FIPS) 201 and Homeland Security Presidential Directive 12 (HSPD-12).  From a technological standpoint, pivotal components in this process include smart card readers. These advanced devices play a crucial role in facilitating the reading and validation of both PIV and CAC credentials. Their primary function is to ensure that only individuals with legitimate credentials gain access to the system. Additionally, the system employs certificate-based authentication mechanisms, relying on cryptographic certificates associated with PIV and CAC cards. These certificates serve as an extra layer of security, verifying the authenticity of the presented credentials and the users wielding them. It is of paramount importance to emphasize the acceptance and electronic verification of Common Access Card (CAC) credentials.  In summary, the meticulous approach taken to accept and electronically verify PIV and CAC credentials underscores the commitment to security within the system. Technological components like smart card readers and certificate-based authentication mechanisms form the foundation of this control enhancement. By ensuring robust identity verification processes, this security infrastructure not only guarantees compliance with the specified standards but also significantly enhances the overall security posture. It plays a critical role in thwarting unauthorized access while facilitating secure, authorized access for users. |

### 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: | |
| Parameter IA-3-1: | |
| Parameter IA-3-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-3 What is the solution and how is it implemented?** |
| --- |
|  |

### IA-4 Identifier Management (L) (M)

The organization manages information system identifiers for users and devices by:

1. Receiving authorization from [*Assignment: organization-defined personnel or roles*] 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: ninety days for user identifiers (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: | |
| Parameter IA-4(a): | |
| Parameter IA-4(d): | |
| Parameter IA-4(e): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |

#### 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: | |
| Parameter IA-4 (4): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-4 (4) What is the solution and how is it implemented?** |
| --- |
|  |

### IA-5 Authenticator Management (L) (M)

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 2. Link <https://pages.nist.gov/800-63-3>.

| **IA-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter IA-5(g): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |
| **Part f** |  |
| **Part g** |  |
| **Part h** |  |
| **Part i** |  |
| **Part j** |  |

#### IA-5 (1) Control Enhancement (L) (M)

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 one (1)*];
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: | |
| Parameter IA-5(1)(a): | |
| Parameter IA-5(1)(b): | |
| Parameter IA-5(1)(d): | |
| Parameter IA-5(1)(e): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-5 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |
| **Part f** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-5 (2) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |

#### 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: | |
| Parameter IA-5(3)-1: | |
| Parameter IA-5(3)-2: | |
| Parameter IA-5(3)-3: | |
| Parameter IA-5(3)-4: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-5 (3) What is the solution and how is it implemented?** |
| --- |
|  |

#### IA-5 (4) Control Enhancement (M)

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*Assignment: organization-defined requirements*].

**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: | |
| Parameter IA-5(4): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-5 (4) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-5 (6) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-5 (7) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter IA-5(11): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-5 (11) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-6 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-7 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-8 What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-8 (1) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-8 (2) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter IA-8(3): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-8 (3) What is the solution and how is it implemented?** |
| --- |
|  |

#### IA-8 (4) Control Enhancement (L) (M) (H)

The information system conforms to FICAM-issued profiles.

| **IA-8 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IA-8 (4) What is the solution and how is it implemented?** |
| --- |
|  |

## Incident Response (IR)

### IR-1 Incident Response Policy and Procedures (L) (M)

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 every three (3) years*]; and
6. Incident response procedures [*FedRAMP Assignment: at least annually*].

| **IR-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter IR-1(a): | |
| Parameter IR-1(b)(1): | |
| Parameter IR-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **IR-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### IR-2 Incident Response Training (L) (M)

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 [*Assignment: organization-defined time period*] 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: | |
| Parameter IR-2(a): | |
| Parameter IR-2(c): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

### IR-3 Incident Response Testing (M)

The organization tests the incident response capability for the information system [*FedRAMP Assignment: at least annually*] using [*FedRAMP Assignment: see additional FedRAMP Requirements and Guidance*] 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: | |
| Parameter IR-3-1: | |
| Parameter IR-3-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-3 What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-3 (2) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: Incident Response Manager | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate   * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | We have established a comprehensive incident handling framework utilizing AWS services. With AWS CloudTrail and Amazon CloudWatch, we actively monitor and detect suspicious activities within our system. In the preparation phase, we have also trained personnel to set up essential monitoring tools, and delineated clear response protocols. Upon detection of any anomalies, our system sends automated alerts to our incident response team, ensuring swift action in line with FedRAMP's requirements. |
| **Part b** | To ensure a holistic response mechanism, our incident handling seamlessly aligns with our contingency planning processes. We've integrated AWS Step Functions to automate and coordinate incident response tasks, ensuring that any incident does not escalate into a broader system or data breach. Moreover, by leveraging Amazon SNS (Simple Notification Service), stakeholders and relevant teams are promptly notified, facilitating quick collaboration and coordination, especially in scenarios demanding rapid response and system recovery. This alignment not only provides swift action during incidents but also ensures that our systems recover efficiently post-incident, minimizing potential disruptions. |
| **Part c** | We continually refine our incident response strategy so thaht we incorporate feedback and insights from past incidents. Post-incident reviews are conducted using tools like AWS Lambda for automated logging and Amazon QuickSight for data visualization. We meticulously analyze the root causes, response times, and the effectiveness of our actions. These lessons learned are then integrated into our training modules and response procedures. Using Amazon S3, we archive these incident reports and evaluations, allowing us to periodically revisit and adjust our strategies. This iterative process ensures our team stays prepared, and our procedures remain in line with FedRAMP's evolving best practices. |

#### 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: Incident Response Manager | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate   * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-4 (1) What is the solution and how is it implemented?** |
| --- |
| To automate the incident handling process, our solution integrates AWS services tailored for enhanced security monitoring and swift response. AWS GuardDuty is our primary tool for intelligent threat detection, which scans for malicious or unauthorized activity. When an anomaly is detected, Amazon CloudWatch Events triggers an automated response, such as isolating affected instances or notifying our security team. Furthermore, AWS Lambda functions are in place for auto-remediation tasks, ensuring quick actions on common threats. All incidents are automatically logged in Amazon CloudTrail, which provides a detailed history of AWS API calls, aiding in post-incident analyses. This automation not only accelerates our incident response but also minimizes potential human errors, aligning with FedRAMP's standards. |

### IR-5 Incident Monitoring (L) (M) (H)

The organization tracks and documents information system security incidents.

| **IR-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Incident Monitoring Coordinator | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate   * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-5 What is the solution and how is it implemented?** |
| --- |
| To ensure the comprehensive tracking and documentation of information system security incidents, we have implemented a centralized incident monitoring solution using AWS CloudWatch combined with AWS CloudTrail. These tools allow us to monitor system events in real-time, capturing and logging any anomalies or potential security incidents. Upon detecting an incident, the system automatically flags it and sends notifications to the Incident Monitoring Coordinator and the security team. We use a dedicated incident management dashboard that categorizes, documents, and archives all incidents, ensuring that all events are tracked systematically. The dashboard also facilitates periodic reviews and reporting, ensuring that all stakeholders are informed and any patterns or trends in security incidents can be analyzed for proactive measures. |

### 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: | |
| Parameter IR-6(a): | |
| Parameter IR-6(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-6 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-7 What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-7 (1) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-7 (2) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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*]; and

**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: | |
| Parameter IR-8(a)(8): | |
| Parameter IR-8(b): | |
| Parameter IR-8(c): | |
| Parameter IR-8(e): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |
| **Part f** |  |

### 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: Information system security officer | |
| Parameter IR-9(b): | |
| Parameter IR-9(f): | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate   * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-9 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | When an contamination event occurs, the first step is to pinpoint the exact data involved in the breach. We utilize AWS CloudTrail combined with Amazon GuardDuty to swiftly trace back to the origins of the spill, determining the nature, sensitivity, and scope of the compromised information. This ensures we know exactly what we're dealing with, enabling a precise and efficient response. |
| **Part b** | When spillage event arise, it's crucial to communicate the issue without worsening the problem. We notify designated emergency response personnel through an independent communication channel, separate from the compromised system. For instance, if an email system experiences a spill, alerts would be sent via secure phone lines or dedicated emergency messaging apps, ensuring that the spill's scope doesn't widen. |
| **Part c** | We use AWS's security group rules and Network Access Control Lists (NACLs), the affected system or component is instantly isolated from the rest of the infrastructure. This prevents further contamination, spread, or unauthorized access while the issue is addressed. |
| **Part d** | Post-isolation, the specific data involved in the spill is removed. AWS Lambda functions are triggered to cleanse storage devices, and Amazon S3 object versioning is employed to revert to a pre-contamination state if necessary. If the data cannot be surgically removed, we have the capability to safely destroy and replace the compromised component. |
| **Part e** | Once the immediate spill is addressed, an expansive review begins wherer we use AWS CloudTrail logs, combined with AWS Config, are scoured to track any lateral movement of the spilled data. This ensures we spot any other systems or components that might have been affected post the initial spillage. |
| **Part f** | Beyond the immediate technical response, our protocol includes a thorough review to determine the spill's cause and prevent future occurrences. This might involve retraining staff, adjusting AWS Identity and Access Management (IAM) policies, or enhancing encryption mechanisms using AWS Key Management Service (KMS) to further safeguard data. |

#### 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: CSO (Chief Security Officer) | |
| Parameter IR-9(1): CSO (Chief Security Officer) | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-9 (1) What is the solution and how is it implemented?** |
| --- |
| The CSO (Chief Security Officer) is tasked with responding to organization-wide information spills. The CSO then reports to the COO and CEO about any important information leaks. The CSO reports to the COO (Chief Operations Officer) and CEO (Chief Executive Officer) by creating a report of the entire data leakage. This document specifies the timestamp of the event(s), the events occurred, the information leaked, the type of leaked information, the severity, how much in percentages was lost or leaked, whom the data pertained to, and how it affects the different areas of the organization by percentage. This document is then reviewed by the CSO and passed on to the COO and the CEO for their own review. The CSO is then in charge of acting upon the events that occurred and executing the data leakage recovery with the Systems Administrator(s) and IT Administrator(s). |

#### IR-9 (2) Control Enhancement (M)

The organization provides information spillage response training [*Assignment: organization- defined frequency*].

| **IR-9 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: CSO (Chief Security Officer) | |
| Parameter IR-9(2): Bi-Quarterly (Every 2 Quarters; e.g., Q1 and Q3) | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-9 (2) What is the solution and how is it implemented?** |
| --- |
| The CSO (Chief Security Officer) is in charge of leading the organization-wide training for information spillage. This training is done in conjunction with the COO (Chief Operations Officer) as it also affects business operations. The information spillage training consists of training sessions spanning three days. The first day is a seminar regarding the types of threats that our specific organization can have (e.g., insider/outsider threats, DoS/DDoS attacks, “phishing”). This teaches the employee what to look out for in their daily life (since it doesn’t only apply to when they’re at work, it could happen anywhere at any time. An employee can have sensitive (company-related) data stored on their personal devices either intentionally, which is a threat, or unintentionally and that’s that data can be stolen/leaked. On the second day, the training consists of actual threat responses. Some examples of this are: forwarding “phish-like” or suspicious emails to a Security Engineer or IT Administrator and reporting to upper management with a threat report (if working as a Security Engineer). The third day consists of a review as well as a security survey that tests every department on certain data security topics. |

#### 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: CSO (Chief Security Officer) | |
| Parameter IR-9(3): Information Spillage Training | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-9 (3) What is the solution and how is it implemented?** |
| --- |
| During the second day of training as explained before, the employees are exposed to many different scenarios involving many different kinds of threats and teach them how to respond to such threats. This includes how to carry on with their work when a certain system goes down. For example, if a backend software developer is working on the website backend services and they’re being threatened, then their job is to help the security engineer generate a report on the threat. Another example would be for a front desk employee to report to management and alert customers that an outage and/or threat is happening at the moment. Upper management (meaning the CSO in conjunction with the COO and Lead Security Engineers) will then be able to handle and mitigate the situation as soon as possible. |

#### 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: CSO (Chief Security Officer) | |
| Parameter IR-9(4): Data Access Security | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **IR-9 (4) What is the solution and how is it implemented?** |
| --- |
| Data access security is enforced through different layers of security. The first layer of security is role management. Every employee at the company has a different role, which applies security access rules. This limits the amount of data that an employee has access to. The second layer is enforced through data version control. This specifically includes identifications of who (user id), when(timestamp) and where (IP and MAC address gathered from our MDM software) a document has been accessed. Following this, data that is part of the organization can only be accessed from the company network (can be accessed via VPN, which allows network monitoring of who is accessing what). Any intruder on the network will be immediately caught by our intrusion detection system (there are various being used in different security teams like Snort and SolarWinds). |

## Maintenance (MA)

### MA-1 System Maintenance Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A system maintenance 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 maintenance policy and associated system maintenance controls; and
2. Reviews and updates the current:
   1. System maintenance policy [*FedRAMP Assignment: at least every three (3) years*]; and
   2. System maintenance procedures [*FedRAMP Assignment: at least annually*].

| **MA-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter MA-1(a): | |
| Parameter MA-1(b)(1): | |
| Parameter MA-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **MA-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Parameter MA-2(c): | |
| Parameter MA-2(f): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MA-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |
| **Part f** |  |

### MA-3 Maintenance Tools (M) (H)

The organization approves, controls, and monitors information system maintenance tools.

| **MA-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Information System security officer | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MA-3 What is the solution and how is it implemented?** |
| --- |
| MA-3, as a critical security control, is instrumental in our efforts to safeguard our organization's sensitive information from unauthorized access. This control is indispensable in mitigating the risk of data breaches that could result from equipment being removed from our facility with company data on it. To effectively implement MA-3, we must first identify all equipment containing organizational information. Subsequently, we need to establish rigorous processes for inspecting or scanning this equipment before it leaves our facility, ensuring that no organizational data remains. Encryption further bolsters our security measures, ensuring that any residual data is protected during equipment removal or disposal. Equally crucial is the implementation of a well-defined approval process for equipment removal, involving our Chief Security Officer (CSO) and Information Security Officer (ISSO) to guarantee comprehensive risk assessment and mitigation. In summary, MA-3 serves as a cornerstone in our compliance with data protection regulations and our commitment to reducing the risk of data breaches, thereby enhancing our overall data security posture.Tools like AWS Secure Eraser are useful for organizations seeking to ensure data compliance and secure data removal from cloud services. These tools provide a solution for deleting data across various AWS services such as EC2 and S3, aligning with the organization's data regulations. This comprehensive data erasure capability not only enhances data security but also assists in meeting regulatory requirements, making it a vital component of a robust data management strategy in the cloud. |

#### 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: IAM System Administrator | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MA-3 (1) What is the solution and how is it implemented?** |
| --- |
| To put this control into action, organizations can establish a protocol for the inspection of maintenance tools. This protocol should comprise several essential steps. Initially, it involves identifying all maintenance tools employed for accessing or maintaining organizational information systems. Following that, organizations should compile a list of authorized modifications permissible for each maintenance tool. Subsequently, a process should be set up to scrutinize these tools for any improper or unauthorized alterations. To ensure the effective execution of these inspections, organizations must provide adequate training to qualified personnel. Finally, a response mechanism should be in place to address any incidents involving the discovery of improper or unauthorized modifications. AWS CloudTrail, AWS Systems Manager Inspector, and AWS Identity and Access Management (IAM) are integral components for securing your AWS infrastructure. AWS CloudTrail serves as a governance and compliance tool, meticulously documenting all API activities within your AWS account, storing the logs in a designated Amazon S3 bucket. This audit trail is invaluable for tracking the timing, actors, and affected resources during any AWS account actions. AWS Systems Manager Inspector, on the other hand, specializes in vulnerability management, automatically evaluating the security posture of your AWS assets and suggesting remedies. It extends its reach to a variety of resources, including Amazon EC2 instances, Amazon RDS databases, and Amazon S3 buckets. Finally, AWS IAM acts as a web service for managing access to AWS resources securely. With IAM, users and groups can be created, permissions assigned, and roles defined – these roles granting permissions to users or groups. When implementing, you can leverage these tools: establish an IAM role exclusively for maintenance personnel, configure CloudTrail to log events into a secure S3 bucket, use Systems Manager Inspector to assess maintenance tools for vulnerabilities, and develop procedures for inspection and remediation. Additionally, centralizing maintenance tools' storage, enforcing check-in/check-out processes, and regularly auditing their use are recommended practices to further fortify your AWS security posture. These combined efforts ensure the safety and integrity. |

#### 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: AWS System Manager | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MA-3 (2) What is the solution and how is it implemented?** |
| --- |
| To reinforce the effectiveness of this control, organizations can adopt a series of strategic measures. These include the implementation of a media management system to meticulously track and oversee media containing diagnostic and test programs, ensuring that all such media is accounted for and subject to regular checks for malicious code. It's essential to institute a continuous scanning process for malware and other malicious code on media, even if prior inspections have taken place, as this ongoing vigilance helps safeguard against evolving threats. Moreover, organizations can bolster security by requiring maintenance personnel to sign non-disclosure agreements (NDAs), underlining the significance of preserving the confidentiality of organizational information. Finally, providing comprehensive security awareness training to maintenance personnel equips them with the knowledge needed to comprehend the unique risks associated with media containing diagnostic and test programs and empowers them to effectively mitigate these risks.  Incorporating this control involves a targeted set of actions. Engaging a managed service provider (MSP) to oversee and manage media containing diagnostic and test programs can ensure regular malware checks and timely application of security patches, enhancing the control's effectiveness. Leveraging AWS Systems Manager for routine scans of media content for malware and malicious code is a strategic move, given its unified perspective on AWS systems and applications and its built-in vulnerability scanning capabilities. Enforcing NDAs among maintenance personnel, encompassing provisions for safeguarding the confidentiality of organizational information, including the details, strengthens security measures further. Lastly, tailoring security awareness training to address the specific risks associated with media containing diagnostic and test programs within the context equips maintenance personnel with the necessary expertise to meet the architecture's security requirements effectively. |

#### 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: Information Security Team | |
| Parameter MA-3(3)(d): | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MA-3 (3) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | In our organization, Our IT staff does a thorough inspection using sophisticated scanning instruments and software diagnostics before any maintenance equipment is suitable for removal or disposal. This makes sure that there are no leftover organizational files, temporary files or even cached data on the device. We have implemented a well-defined system for categorizing equipment, ensuring that each piece is clearly labeled and categorized. This helps in distinguishing between maintenance equipment and devices containing organizational information. We regularly update and monitor our equipment inventories, keeping accurate records of each item's status and location in order to preserve transparency and control. |
| **Part b** | We act quickly when questions or concerns arise regarding the potential presence of organizational data on the equipment as a result of our advanced verification process. We use AWS secure erasure tools for sanitization, which repeatedly overwrite storage sectors with randomized data, making it impossible to recover the original data. However, if the data on the equipment cannot be reliably cleaned up or if it is reached its end-of-life phase, we choose physical destruction. This involves physically dismantled of essential components like storage device, data chips and drives are subjected to degaussing and then shredded, ensuring an absolute defense against any potential data recovery efforts. |
| **Part c** | The organization has a protocol which enables the old equipment to retain within the organization to use by a different team to avoid losing the equipemnt to wasteage and use the equipmen to its fuk extent. In situations where it cannot be used any longer then necessary actions would be taken according to MA-3(3) part b. |
| **Part d** | In the case where the organization decides to remove the equipment, it would go through several leves of approvals for the exemption to be removed. The checks would include to identify the need for removing equipment, accessing the risks, encryption of the data if it does contain any official data and auditing. Once teh equipment go throughs these stages it would be approved for exemption to be removed. All these activities would be tracked through a custom inhouse web application which keeps tracks of everything. |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MA-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MA-4 (2) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MA-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

#### MA-5 (1) Control Enhancement (L) (M)

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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MA-5 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Parameter MA-6(1): | |
| Parameter MA-6(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MA-6 What is the solution and how is it implemented?** |
| --- |
|  |

## Media Protection (MP)

### MP-1 Media Protection Policy and Procedures (L) (M)

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 every three (3) years*]; and
   2. Media protection procedures [*FedRAMP Assignment: at least annually*].

| **MP-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter MP-1(a): | |
| Parameter MP-1(b)(1): | |
| Parameter MP-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **MP-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### MP-2 Media Access (L) (M)

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

| **MP-2** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter MP-2-1: | |
| Parameter MP-2-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MP-2 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter MP-3(b)-1: | |
| Parameter MP-3(b)-2: Not applicable | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MP-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Parameter MP-4(a)-1: | |
| Parameter MP-4(a)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MP-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Parameter MP-5(a)-1: | |
| Parameter MP-5(a)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MP-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MP-5 (4) What is the solution and how is it implemented?** |
| --- |
|  |

### MP-6 Media Sanitization and Disposal (L) (M)

The organization:

1. Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] 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: | |
| Parameter MP-6(a)-1: | |
| Parameter MP-6(a)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MP-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### MP-6 (2) Control Enhancement (M)

The organization tests sanitization equipment and procedures [*FedRAMP Assignment: at least annually*] 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: | |
| Parameter MP-6(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MP-6 (2) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter MP-7-1: | |
| Parameter MP-7-2: | |
| Parameter MP-7-3: | |
| Parameter MP-7-4: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MP-7 What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **MP-7 (1) is the solution and how is it implemented?** |
| --- |
|  |

## Physical and Environmental Protection (PE)

### PE-1 Physical and Environmental Protection Policy and Procedures (L) (M)

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 every three (3) years*]; and
   2. Physical and environmental protection procedures [*FedRAMP Assignment: at least annually*].

| **PE-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter PE-1(a): | |
| Parameter PE-1(b)(1): | |
| Parameter PE-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **PE-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### PE-2 Physical Access Authorizations (L) (M)

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 annually*]; and
4. Removes individuals from the facility access list when access is no longer required.

| **PE-2** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter PE-2(c): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |

### 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*];
2. Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*];
3. Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible;
4. Escorts visitors and monitors visitor activity [*FedRAMP Assignment: in all circumstances within restricted access area where the information system resides*];
5. Secures keys, combinations, and other physical access devices;
6. Inventories [*Assignment: organization-defined physical access devices*] every [*FedRAMP Assignment: at least annually*]; and
7. 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: | |
| Parameter PE-3(a): | |
| Parameter PE-3(a)(2): | |
| Parameter PE-3(b): | |
| Parameter PE-3(c): | |
| Parameter PE-3(d): | |
| Parameter PE-3(f)-1: | |
| Parameter PE-3(f)-2: | |
| Parameter PE-3(g): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |
| **Part f** |  |
| **Part g** |  |

### 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: | |
| Parameter PE-4-1: | |
| Parameter PE-4-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-4 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-5 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter PE-6(b)-1: | |
| Parameter PE-6(b)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

#### PE-6 (1) Control Enhancement (M) (H)

The organization monitors physical intrusion alarms and surveillance equipment.

| **PE-6 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-6 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter PE-8(a): | |
| Parameter PE-8(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-9 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter PE-10(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-10 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

### 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: | |
| Parameter PE-11: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-11 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-12 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-13 What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter PE-13(2)-1: | |
| Parameter PE-13(2)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-13 (2) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-13 (3) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter PE-14(a): | |
| Parameter PE-14(b): | |
| Parameter PE-14(b) Additional: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-14 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-14 (2) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-15 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter PE-16: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-16 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter PE-17(a): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PE-17 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

## Planning (PL)

### PL-1 Security Planning Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A security 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 security planning policy and associated security planning controls; and
2. Reviews and updates the current:
   1. Security planning policy [*FedRAMP Assignment: at least every three (3) years*]; and
   2. Security planning procedures [*FedRAMP Assignment: at least annually*].

| **PL-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter PL-1(a): | |
| Parameter PL-1(b)(1): | |
| Parameter PL-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **PL-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### PL-2 System Security Plan (L) (M) (H)

The organization:

1. Develops a security plan for the information system that:
   1. Is consistent with the organization’s enterprise architecture;
   2. Explicitly defines the authorization boundary for the system;
   3. Describes the operational context of the information system in terms of missions and business processes;
   4. Provides the security categorization of the information system including supporting rationale;
   5. Describes the operational environment for the information system and relationships with or connections to other information;
   6. Provides an overview of the security requirements for the system;
   7. Identifies any relevant overlays, if applicable;
   8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
   9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
2. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*];
3. Reviews the security plan for the information system [*FedRAMP Assignment: at least annually*];
4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

| **PL-2** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Chief Security Officer | |
| Parameter PL-2(b): | |
| Parameter PL-2(c): | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PL-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | The development of a security plan for our information system is a meticulous process. It starts with ensuring that the plan aligns seamlessly with our organization's enterprise architecture, enabling the efficient operation of our services. The plan explicitly defines the authorization boundary, outlines the operational context in terms of missions and business processes, and categorizes the system with supporting rationale, determining the sensitivity and impact of potential breaches. We detail the operational environment, including relationships with other systems, and highlight the security requirements, ensuring comprehensive protection. If applicable, relevant overlays are identified. The plan describes existing and planned security controls, with a rationale for any tailoring decisions, all culminating in a thorough review and approval by the authorizing official or their designated representative before implementation, assuring a secure and compliant information system. |
| **Part b** | Distributing copies of the security plan and effectively communicating subsequent changes to the plan is a critical aspect of our security strategy. We ensure that the security plan is shared with organization-defined personnel or roles, allowing for a broad understanding of our security measures. Furthermore, any updates or modifications to the plan are promptly communicated to these designated individuals or roles to maintain awareness and ensure that our security strategy remains up-to-date and responsive to evolving threats and requirements. This communication process is integral to our overall security posture. An internal communication is made every 2 months to make sure that everyone is aware of it frequently. |
| **Part c** | The security plan would be reviewed by the CSO and all other required personnel annually and if any changes are required for specific sector, they would be made in the annual meeting and some new services may be added in the year middle which would cause a disturbance in the existing policies and security framework, in those cases security plan may be modified by the CSO and respective personnel to make sure everything is under compliance. |
| **Part d** |  |
| **Part e** |  |

#### 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: CSO | |
| Parameter PL-2(3): | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PL-2 (3) What is the solution and how is it implemented?** |
| --- |
| The solution entails designating responsible parties, including regular meetings led by the Chief Security Officer (CSO), to plan and coordinate security-related activities. These meetings serve as a platform for discussions, policy adjustments, and potential updates to security frameworks. They are conducted on a quarterly basis, and active participation from all relevant stakeholders is mandatory to ensure alignment and understanding across the organization. This approach fosters ongoing communication and collaboration, enhancing the organization's ability to reduce the impact of security activities on other entities while maintaining a strong security posture. |

### PL-4 Rules of Behavior (L) (M)

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: at least every three (3) years*]; 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: | |
| Parameter PL-4(c): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PL-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PL-4 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: Chief Security Officer (CSO) | |
| Parameter PL-8(b): Bi-Quarterly | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):   * Service Provider Corporate   ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PL-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | *NetShield’s* information security architecture is composed of several crucial components. In regards to protecting our user data, the CSO (Chief Security Officer) has implemented a set of policies to prevent data leakage. These policies also ensure that if an insider threat were to occur, everything regarding that threat is logged by our log service. This would include who did it internally (user ID), timestamp, what service it was, as well as which services, files or directories were mutated or viewed. This service logging system is serviced by two AWS services: AWS CloudWatch (analyze logs and metrics of our services) and AWS CloudTrail (records user actions and helps manage user logs and even compliance). These two AWS services are running 24/7 monitoring our other services running on our 1 account. We also utilize Amazon VPC (Virtual Private Cloud) Flow Logs that monitor the IP traffic between our services (including CloudWatch). All of these AWS services are third-party services that our company relies on for logging. These services are crucial for our company since we have to make sure that our data is intact, and if it isn’t we know who or what caused it.  Besides logging, we use Amazon Detective and Amazon GuardDuty to effectively identify any malicious threats that might be going on in our system. Amazon GuardDuty is very effective for us since it can monitor all of our hosted services (e.g., S3, clusters, containers, etc.) and it can detect when unusual activity is happening (e.g., odd API calls from unrecognized IP’s, DDoS attacks, etc.). Amazon Detective collects the log data from Amazon VPC Flow Logs and helps us quickly identify where the security issue is from the log(s) you choose to analyze. We also use Amazon Inspector to continually make sure that our hosted services are up to date and also helps us find current vulnerabilities so that we can update them when needed.  Finally, for role management and network security for our services, we use AWS IAM (Identity and Access Management) for role-based access into our services and AWS Network Firewall to be able to protect our hosted services by whitelisting only certain subnets. This is important because we only allow subnets that are in our building. If an employee is working remotely, they have to tunnel into our network (using a VPN) to be able to access these services. |
| **Part b** | Our information security architecture is updated every two quarters to ensure that every component is up to date. When handling very critical user data, it’s important to keep all software and components updated because of security threats. If a security threat were to be found on one of our services, we would either update it to the latest hotfix immediately (not waiting for another two quarters) or shut the service off if the threat applies to us and there’s no update yet. The company cannot afford to lose or have mutated user data because of insider/outsider threats done through vulnerabilities on our services. |
| **Part c** | Any time that our information security architecture is changed it is reflected on our security plan. This is reported to the CSO (Chief Security Officer) and then completed by the CSO. The CSO is in charge of updating the company’s security plan since the plan applies to the company as a whole. If there are parts changed in our architecture that apply to CONOPS and/or organizational procurements/acquisitions, it will be updated as well. These updates are completed right after the information security system has been updated so that all records and policies are up to date. |

## Personnel Security (PS)

### PS-1 Personnel Security Policy and Procedures (L) (M)

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 every three (3) years*]; and
   2. Personnel security procedures [*FedRAMP Assignment: at least annually*].

| **PS-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter PS-1(a): | |
| Parameter PS-1(b)(1): | |
| Parameter PS-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **PS-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### PS-2 Position Categorization (L) (M)

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 every three (3) years*].

| **PS-2** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Chief Information Security Officer (CISO) | |
| Parameter PS-2(c): Every 3 years | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate Service Provider System Specific   * Service Provider Hybrid (Corporate and System Specific)   ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PS-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | We have implemented a comprehensive risk assessment matrix that aligns with AWS's best practices for security and compliance. Leveraging the AWS Identity and Access Management (IAM) framework, each role or position within the organization is assigned a risk designation based on its access to sensitive data, operational capabilities, and overall impact on the system's integrity. This risk designation utilizes a combination of automated AWS Config rules and manual evaluations to determine the level of potential exposure and risk associated with each position. |
| **Part b** | Once risk designations are in place, we have outlined rigorous screening criteria for individuals vying for these positions. These criteria are based on the AWS Best Practices for IAM and involve both technical and behavioral evaluations. For roles with elevated privileges or access to critical data, AWS's MFA - Multi-Factor Authentication is mandated, and users are screened for their understanding of AWS's shared responsibility model. Additionally, background checks, training histories, and other relevant evaluations are conducted in alignment with the risk associated with each role. |
| **Part c** | To ensure the continuous relevance of our risk designations, we have integrated AWS CloudWatch along with custom Lambda functions to provide automated alerts for any deviations or anomalies in role-based activities. This allows for real-time monitoring and quick adjustments. Additionally, in adherence to FedRAMP's guidelines, every three years, our security and HR teams collaboratively review these designations using AWS's well-architected framework as a baseline. This triennial review, combined with AWS's continuously evolving security services, ensures our position risk designations remain updated and in line with the most current threat landscape. |

### 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: | |
| Parameter PS-3(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PS-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Parameter PS-3 (3)(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PS-3 (3) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### PS-4 Personnel Termination (L) (M)

The organization, upon termination of individual employment:

1. Disables information system access within [*FedRAMP Assignment: same day*];
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: | |
| Parameter PS-4(a): | |
| Parameter PS-4(c): | |
| Parameter PS-4(f)-1: | |
| Parameter PS-4(f)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PS-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |
| **Part f** |  |

### PS-5 Personnel Transfer (L) (M)

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 [*Assignment: organization-defined time period following the formal transfer action*];
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: within five days of the formal transfer action (DoD 24 hours)*].

| **PS-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter PS-5(b)-1: | |
| Parameter PS-5(b)-2: | |
| Parameter PS-5(d)-1: | |
| Parameter PS-5(d)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PS-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |

### PS-6 Access Agreements (L) (M)

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*].

| **PS-6** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter PS-6(b): | |
| Parameter PS-6(c)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PS-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

### PS-7 Third-Party Personnel Security (L) (M)

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: same day*]; and
5. Monitors provider compliance.

| **PS-7** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter PS-7(d)-1: | |
| Parameter PS-7(d)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PS-7 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |

### PS-8 Personnel Sanctions (L) (M)

The organization:

1. Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
2. Notifies [A*ssignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

| **PS-8** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter PS-8(b)-1: | |
| Parameter PS-8(b)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **PS-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

## Risk Assessment (RA)

### RA-1 Risk Assessment Policy and Procedures (L) (M)

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 every three (3) years*]; and
   2. Risk assessment procedures [*FedRAMP Assignment: at least annually*].

| **RA-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter RA-1(a): | |
| Parameter RA-1(b)(1): | |
| Parameter RA-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **RA-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **RA-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

### RA-3 Risk Assessment (L) (M)

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: | |
| Parameter RA-3(b): | |
| Parameter RA-3(c): | |
| Parameter RA-3(d): | |
| Parameter RA-3(e): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **RA-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |

### 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**

[https://www.FedRAMP.gov/documents/](https://www.fedramp.gov/documents/)

| **RA-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Chief Security Officer (CSO) | |
| Parameter RA-5(a): monthly operating system/infrastructure; monthly web applications and databases | |
| Parameter RA-5(d): 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 | |
| Parameter RA-5(e): Organization defined personnel/role: Chief Security Officer(CSO) | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **RA-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | The organization's approach to vulnerability management entails regular scans of its information system and hosted applications, carried out on a monthly basis, with additional scans triggered in response to newly discovered vulnerabilities. An accredited independent assessor conducts an annual assessment encompassing operating systems, infrastructure, web applications, and databases. To translate this requirement, the organization can leverage a suite of AWS services:  Firstly, AWS Systems Manager Vulnerability Scanner is employed for comprehensive vulnerability scans, including operating systems, applications, and databases. These scans can be scheduled to run periodically, such as on a monthly basis or whenever new vulnerabilities are detected. Secondly, AWS Inspector automates security assessments of AWS resources, spanning operating systems, applications, and databases, with a focus on identifying vulnerabilities, malware, and security risks. Finally, the AWS Penetration Testing Service offers on-demand penetration testing to identify vulnerabilities and misconfigurations susceptible to exploitation by potential attackers.  Complementing the use of AWS services, the organization can institute a set of procedures to ensure the efficacy of vulnerability scanning. This includes formulating a vulnerability scanning policy that defines the scanning scope, frequency, and procedures for addressing identified vulnerabilities. Critical systems and applications are prioritized for more frequent scans. Regular review of scan results, coupled with swift remediation efforts, such as applying security patches or revising configurations, is emphasized. The organization also commits to monitoring security advisories and bulletins for newly discovered vulnerabilities affecting the system and applications, triggering scans and prompt remediation in response. By adhering to these procedures, the organization guarantees it is subjected to regular vulnerability assessments and that any identified vulnerabilities are addressed promptly. |
| **Part b** | The organization has adopted a strategy that prioritizes the utilization of vulnerability scanning tools and techniques aimed at fostering interoperability among these tools and automating various elements of the vulnerability management process. This strategy is guided by adherence to established standards, focusing on three key areas: the enumeration of platforms, identification of software flaws, and detection of improper configurations; the formatting of checklists and test procedures to enhance transparency and comprehensibility; and the assessment of the impact of vulnerabilities, thereby gaining a deeper understanding of their potential consequences.  To put this requirement into practice, the organization can effectively harness a combination of AWS services designed to align with these principles. AWS Systems Manager Vulnerability Scanner is instrumental in this approach, offering support for the Open Vulnerability Assessment Language (OVAL), a recognized standard format for defining vulnerabilities that facilitates seamless information exchange among various scanning tools. Additionally, AWS Inspector is a valuable service that adheres to OVAL while also accommodating additional vulnerability standards such as the Common Vulnerabilities and Exposures (CVE) list. Furthermore, the AWS Penetration Testing Service plays a vital role in conducting penetration tests that adhere to widely-accepted vulnerability scanning methodologies, including those outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).  Beyond the adoption of AWS services, the organization is encouraged to implement a set of procedures designed to ensure the interoperability and automation of its vulnerability scanning tools and techniques. These include the development and execution of a comprehensive vulnerability scanning policy and accompanying procedures that expressly define the standards to be employed in the vulnerability scanning process, with a particular emphasis on the use of the OVAL standard. Careful selection of vulnerability scanning tools that align with OVAL and other pertinent standards is paramount, as is the meticulous configuration of these scanning tools to enable the seamless exchange of information via OVAL. Furthermore, the establishment of automated protocols for addressing identified vulnerabilities, encompassing actions such as the application of security patches, configuration updates, and the implementation of compensating controls, is vital to the success of the vulnerability management process. |
| **Part c** | The organization has established a comprehensive protocol for analyzing vulnerability scan reports and the results of security control assessments. This protocol serves a dual purpose: the identification and prioritization of vulnerabilities, and the formulation and execution of remediation plans. When integrating this requirement, the organization can seamlessly incorporate a combination of AWS services:  AWS Systems Manager Vulnerability Scanner provides vulnerability scan reports that include essential details about identified vulnerabilities, their severity levels, and the recommended steps for remediation. Likewise, AWS Inspector delivers vulnerability scan reports and extends its capabilities to offer comprehensive reports on the security status of AWS resources. Notably, AWS Security Hub acts as a central hub for consolidating security findings from various AWS services, including AWS Systems Manager Vulnerability Scanner and AWS Inspector. This consolidation simplifies the organization's ability to analyze vulnerability scan reports and security control assessment results.  In addition to the utilization of AWS services, the organization can establish a series of procedures to ensure the effective analysis of vulnerability scan reports and security control assessment outcomes. This includes the development and implementation of a vulnerability analysis process and corresponding procedures, which explicitly outline the methodology for analyzing vulnerability scan reports, prioritizing identified vulnerabilities, and devising and executing remediation plans. The organization can further enhance its approach by designating a qualified team responsible for vulnerability analysis, equipped with the requisite skills and knowledge to comprehensively understand and evaluate vulnerability scan reports. Regular reviews and updates of the vulnerability analysis process and its associated procedures should also be conducted to maintain effectiveness and alignment with the evolving security needs of the organization. By adhering to these procedures, the organization can ensure the systematic and effective analysis of vulnerability scan reports and security control assessment results, thereby guaranteeing the identification, prioritization, and prompt remediation of vulnerabilities. |
| **Part d** | Within the realm of vulnerability remediation, the organization diligently adheres to a risk-based approach, addressing valid vulnerabilities based on the findings of its internal risk assessment. The Federal Risk and Authorization Management Program (FedRAMP) prescribes distinct deadlines for remedying vulnerabilities, classifying them by severity levels: high-risk vulnerabilities require resolution within 30 days of discovery, moderate-risk vulnerabilities within 90 days, and low-risk vulnerabilities within 180 days. To adapt this mandate, the organization can seamlessly incorporate a combination of AWS services.  Among these services, AWS Systems Manager Patch Manager proves invaluable, offering the capability to automatically deploy security patches to AWS systems, mitigating the risks associated with human error and ensuring the timely application of essential patches. Additionally, AWS Systems Manager Parameter Store serves as a centralized repository for storing and managing security configuration parameters, ensuring uniformity in security configurations across all AWS systems. Further bolstering these efforts, AWS Systems Manager Automation empowers the organization to automate various tasks associated with vulnerability remediation, including the deployment of security patches and updates to security configurations.  Complementing these AWS services, the organization can implement specific procedures to optimize the effectiveness of vulnerability remediation. This involves the development and implementation of a well-structured vulnerability remediation process and associated procedures, meticulously defining vulnerability prioritization, the formulation and execution of remediation plans, and verification procedures for remediation completion. Responsibility for vulnerability remediation is assigned to a qualified team equipped with the necessary skills and knowledge for efficient and effective vulnerability mitigation. Regular reviews and updates of the vulnerability remediation process and associated procedures are essential to maintain their effectiveness and ensure alignment with the organization's evolving security requirements. |
| **Part e** | In alignment with the requirement, the organization actively disseminates information acquired through the vulnerability scanning process and security control assessments to designated personnel or roles within the organization. This information sharing is instrumental in addressing systemic weaknesses or deficiencies, essentially aiding in the mitigation of similar vulnerabilities across other information systems. Among the recipients of this information are all Authorizing Officials and FedRAMP for JAB authorizations, ensuring a comprehensive approach to vulnerability management.  To fulfill this mandate, the organization can deploy a variety of methods within the AWS environment. Firstly, the creation of a vulnerability tracking system serves as a crucial tool. This system effectively stores and manages data pertaining to vulnerabilities, including their type, severity, and the remediation steps undertaken. This data can then be shared with personnel or roles defined by the organization, facilitating their identification and remediation of analogous vulnerabilities in other information systems. Regular vulnerability management meetings are another valuable avenue for sharing such information. These meetings become a platform for disseminating details on vulnerabilities and deliberating on remediation plans. Attended by personnel or roles entrusted with responsibilities in vulnerability management, security, and other pertinent areas, these meetings play a pivotal role in the information-sharing process.  In addition to the use of AWS services, the organization can enact a set of procedures to ensure the effective sharing of information derived from the vulnerability scanning process and security control assessments. This encompasses the formulation and implementation of a vulnerability information sharing policy and associated procedures, explicitly defining the methodologies through which vulnerability information will be shared with personnel or roles designated by the organization. Furthermore, a proactive approach involves the identification of the specific personnel or roles within the organization responsible for receiving and taking action on vulnerability information. These individuals or roles should possess the requisite skills and knowledge to competently identify and address vulnerabilities. Routine reviews and updates of the vulnerability information sharing policy and its corresponding procedures are essential in maintaining the policy's efficacy and aligning it with the evolving security requirements of the organization.  Further considerations for effective information sharing include leveraging AWS Security Hub for centralized and secure sharing of vulnerability information and the utilization of AWS Identity and Access Management (IAM) for controlling access to vulnerability data. Additionally, the implementation of AWS encryption for both data at rest and data in transit is fundamental in safeguarding vulnerability information against unauthorized access. |

#### 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: Chief Security Officer (CSO) | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **RA-5 (1) What is the solution and how is it implemented?** |
| --- |
| In accordance with this requirement, the organization deploys vulnerability scanning tools equipped with the essential capability to promptly update the roster of information system vulnerabilities slated for scanning. This capability proves indispensable due to the continuous emergence of new vulnerabilities, necessitating swift identification and scanning. To seamlessly incorporate this requirement, the organization can employ a diverse array of methods.  One effective method involves the utilization of AWS Systems Manager Vulnerability Scanner, which harnesses the National Vulnerability Database (NVD) to pinpoint and scan for vulnerabilities. The NVD undergoes regular updates, ensuring that AWS Systems Manager Vulnerability Scanner automatically scans for newly discovered vulnerabilities as soon as they are added to the database. Similarly, AWS Inspector leverages the NVD to identify and scan for vulnerabilities, offering the added benefit of customization for scanning vulnerabilities specific to certain operating systems, applications, and databases. Furthermore, the organization can opt for third-party vulnerability scanning tools, which often offer the feature of automatic list updates, allowing for the swift integration of new vulnerabilities into the scanning process.  Complementing the use of AWS services, the organization can put in place a set of procedures to guarantee the readiness of its vulnerability scanning tools to update the list of information system vulnerabilities slated for scanning. This includes the development and implementation of a vulnerability scanning tool update policy and accompanying procedures. This policy delineates how vulnerability scanning tools will be updated and establishes the frequency of updates. Responsibility for updating these tools is entrusted to a qualified team equipped with the necessary skills and knowledge to execute updates in a timely and effective manner. Periodic reviews and updates of the vulnerability scanning tool update policy and associated procedures are paramount in maintaining their effectiveness and alignment with the evolving security requirements of the organization.  Moreover, additional considerations for updating vulnerability scanning tools within a 911 cloud architecture hosted on AWS encompass leveraging AWS Systems Manager Parameter Store to facilitate the storage and management of vulnerability scanning tool configuration parameters. This simplifies the process of updating these tools with new lists of vulnerabilities to be scanned. Furthermore, AWS Systems Manager Automation can be instrumental in automating the update process for vulnerability scanning tools, optimizing efficiency and effectiveness. Thorough testing of any updates to these tools before deploying them to production environments is essential in preventing unintended consequences.  Through the careful integration of these considerations and procedures, the organization ensures that its vulnerability scanning tools remain primed to swiftly update the list of information system vulnerabilities to be scanned, facilitating the immediate scanning of newly discovered vulnerabilities. |

#### 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: Security Team | |
| Parameter RA-5(2): | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **RA-5 (2) What is the solution and how is it implemented?** |
| --- |
| Our organization has established a robust vulnerability scanning and update process. Our security team regularly scan our application components using automated tools like AWS Inspector and third-party solutions. These kinds of scans are automated and it is scheduled on each month’s end date . In the event of unexpected application behavior or major incidents that could threaten our system, security team conduct unscheduled scans for proactive threat detection. When new vulnerabilities are identified, then we follow a predefined process for assessment, prioritization, and remediation. Also, we have maintained a detail document where we noted down all the actions that has been taken. Prior to initiating a new scan, we ensure all necessary updates and patches are deployed to mitigate known vulnerabilities. To enhance the tool's effectiveness, our security team receives quarterly training so that they get better understanding on tool’s functionalities and dependencies and also they can get familiar with any new updates . |

#### 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: Security Team | |
| Implementation Status (check all that apply):  ✓Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **RA-5 (3) What is the solution and how is it implemented?** |
| --- |
| Our application is using AWS backend, so we are utilizing Amazon Inspector, an automated security assessment service. To maintain security and compliance throughout the development and deployment lifecycle, Amazon Inspector automatically assesses our applications and discover vulnerabilities and deviations from best practices. This service efficiently scans our AWS infrastructure, including EC2 instances, producing detailed vulnerability reports that are crucial for our security efforts. Security Team , analyzed vulnerabilities and prioritized it based on their risk scores and it helps IT team to find solution of critical issues first. In addition to Amazon Inspector, in our organization we also use AWS services like CloudTrail for monitoring and IAM for access management. This tactic enhances the security and compliance of our application while showcasing the breadth and depth of our vulnerability scanning coverage. |

#### 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: Security Administrator | |
| Parameter RA-5(5)-1: Access authorization | |
| Parameter RA-5(5)-2: Operating Systems, databases and web applications | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ✓ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **RA-5 (5) What is the solution and how is it implemented?** |
| --- |
| In our organization, Security Administrator is responsible of implementing privileged access authorization for our application. The Security Administrator utilizes AWS Identity and Access Management (IAM) to manage and control access to our operating systems, databases, and web applications. Only trusted individuals within this specialized group can access and manage these sensitive components. To ensure they have the necessary security clearances and training, these specialists go through a screening process. In the context of vulnerability scanning, IAM empowers our vulnerability assessment specialists to conduct scans and monitor system components effectively. When vulnerabilities are discovered, our security staff responds quickly to make sure that the reporting, access management, and problem-solving procedures all function properly. |

#### 

#### 

#### 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: Security Administrator | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ✓ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **RA-5 (6) What is the solution and how is it implemented?** |
| --- |
| Our organization has successfully implemented an automated system to compare vulnerability scan results over time for our application. We use AWS Inspector, an automated security assessment service, to conduct regular scans of our AWS infrastructure and application components. The results of these scans are systematically collected and stored in a dedicated repository, establishing a comprehensive database of vulnerabilities. AWS Inspector, in combination with AWS CloudWatch and custom monitoring scripts are utilized to analyze this vulnerability data, enabling us to identify trends and patterns in vulnerabilities over time. When the system detects these trends, automated alerts are triggered, and detailed reports are generated, enabling our security team to proactively address and take appropriate actions to mitigate the vulnerabilities. |

#### 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: Security Team | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ✓ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **RA-5 (8) What is the solution and how is it implemented?** |
| --- |
| Our organization has established a systematic process for reviewing historical audit logs to determine whether vulnerabilities, specifically those classified as high based on NIST criteria have been exploited in the past. Our security staff carefully reviews the historical audit logs, paying close attention to high vulnerability scan findings that are categorized in accordance with NIST's strict standards. Our efficient management and analysis of these logs is made possible using AWS CloudWatch and customized scripts. Our team carefully compares high vulnerability findings from these rigorous tests with earlier logs, looking for any indication of previous exploitation or security incidents connected to these vulnerabilities. If an exploitation is found, our security team immediately starts mitigation procedures, such as the installation of security patches, configuration adjustment, and the implementation of essential security updates. |

## System and Services Acquisition (SA)

### SA-1 System and Services Acquisition Policy and Procedures (L) (M)

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 every three (3) years*]; and
   2. System and services acquisition procedures [*FedRAMP Assignment: at least annually*].

| **SA-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter SA-1(a): | |
| Parameter SA-1(b)(1): | |
| Parameter SA-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **SA-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

### 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: Software Engineering Manager | |
| Parameter SA-3(a): Jira, GitHub and Jenkins CI/CD | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific   * Service Provider Hybrid (Corporate and System Specific)   ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | For our Software Development Lifecycle (SDLC) we use a conjunction of systems to help us achieve a smooth development flow. These systems are:   1. Jira (for ticket tracking/assignments) – Planning & Project Design 2. GitHub (for code history) – Implementation 3. Jenkins CI/CD (for automating testing and deployment tasks) – Testing & Deployment   These are the high-level applications used for our SDLC. In between these systems there exist people like Quality Assurance (QA), software developers, development operations developers (DevOps), and project managers that each contribute to these systems. For example, QA mainly reviews GitHub commits and sends it back to developers (as well as use other tools for testing on their own), project managers use Jira to assign tickets and tasks to certain developers and DevOps developers use GitHub along with Jenkins to be able to automate and deploy builds correctly (they might use platforms used by the QA people as well to test final builds). |
| **Part b** | The Software Engineering Manager (SEM) is in charge of assigning and keeping track of security roles, SDLC tools as well as team-dependent responsibilities. The Software Engineering Manager is in charge of meeting with team leads each week to be able to determine next steps, blockers and high-level tracking of tasks for each individual team-related project. The SEM is also in charge of enforcing security policies by separating teams and assigning the specific needed resources. These policies are placed by the CSO (Chief Security Officer) so that the SEM can then enforce them on all the different (software) teams and assign the correct policies to each team. The SEM keeps track of all the different team-related security policies and resources being given to them and are approved by the CSO. |
| **Part c** | The Software Engineering Manager (SEM) is in charge of assigning all the different security policies and roles written by the CSO (Chief Security Officer). The SEM then enforces these policies and assigns roles to their teams based on these policies (e.g., there might be a team working on security-related research/tooling and needs more access to things while there’s a team working on just UI-related development for our main software). Before starting any project, the team lead for the team leading that project meets with the SEM to configure needed resources and security policies. This is done since our app deals with emergencies and critical PII (Personal Identifiable Information) data. |
| **Part d** | Once the Software Engineering Manager (SEM) meets with all the team leads for their weekly meeting and/or for new project setup requirements, all of the security policies in place will be applied to each step of the Software Development Lifecycle (SDLC). For example, we have a team working on low-level security for our application software. That team needs resources like having access to other parts of the application (frontend and backend service access), while a team writing UI only needs access to the frontend code. There are other tool permissions like GitHub permissions (that are also assigned at a high level by the SEM along with the individual team lead) that allows different teams to have (push and pull) access to their own and other repositories. As for Jenkins, not every team in the software engineering department will have access to it or will have permission to test the CI/CD pipeline of our application. These rules are put in-place to mitigate security and development issues (e.g., if a developer from the frontend team accidentally pushes a commit to a ‘main’ branch of a backend service branch or if they force-push to main without approval). These rules are in-place to protect both the SDLC pipeline as well as the health and state of our software. |

### 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.

**SA-4 Additional FedRAMP Requirements and Guidance:**

**Requirement**: The service provider must comply with Federal Acquisition Regulation (FAR) Subpart 7.103, and Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (Pub. L. 115-232), and FAR Subpart 4.21, which implements Section 889 (as well as any added updates related to FISMA to address security concerns in the system acquisitions process).

**Guidance**: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.   
See <https://www.niap-ccevs.org/Product/>

| **SA-4** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |
| **Part f** |  |
| **Part g** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-4 (1) What is the solution and how is it implemented?** |
| --- |
|  |

#### SA-4 (2) Control Enhancement (L) (M)

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): to include security-relevant external system interfaces, and high-level design*]; [*Assignment: organization-defined design/implementation information*] at [*Assignment: organization-defined level of detail*].

| **SA-4 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter SA-4-1: | |
| Parameter SA-4-2: | |
| Parameter SA-4-3: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-4 (2) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter SA-4(8): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-4 (8) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-4 (9) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-4 (10) What is the solution and how is it implemented?** |
| --- |
|  |

### SA-5 Information System Documentation (L) (M)

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 [*Assignment: organization-defined personnel or roles)*].

| **SA-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter SA-5(c): | |
| Parameter SA-5(e): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-8 What is the solution and how is it implemented?** |
| --- |
|  |

### 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](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: | |
| Parameter SA-9(a): | |
| Parameter SA-9(c): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-9 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

#### 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: | |
| Parameter SA-9(1)(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-9 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

#### 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: | |
| Parameter SA-9(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-9 (2) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter SA-9(4)-1: | |
| Parameter SA-9(4)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-9 (4) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter SA-9(5)-1: | |
| Parameter SA-9(5)-2: | |
| Parameter SA-9(5)-3: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-9 (5) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: DevOps Team Lead | |
| Parameter SA-10(a): Development, implementation and operation | |
| Parameter SA-10(b): Configuration Items like Software code repositories, build and deployment scripts, infrastructure as code files, configuration files | |
| Parameter SA-10(e): Security flaws tracking and reporting to team lead | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate   * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-10 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | **Configuration Management during Lifecycle**  1. Personnel:   1. The Configuration Manager oversees the entire configuration process across the lifecycle. 2. The DevOps Team ensures that configuration management practices are integrated into daily operations.   2. Technology:   1. In-House Technologies:    1. Version control systems like Git are used for managing changes.    2. CI/CD pipelines automate build and deployment.    3. i. Configuration management tools like Ansible are integrated for managing infrastructure and application configurations.   The development team uses Git for version control, ensuring that all changes are tracked. Automated CI/CD pipelines, managed by tools like Jenkins or GitHub Actions, enable consistent deployment practices across environments. |
| **Part b** | **Documenting and Controlling Changes**   1. Personnel:    1. Developers:       1. Document change rationales in version control commits.       2. Engage in peer reviews for each change.    2. Change Management Board:       1. Evaluates and approves significant changes.       2. Assesses changes for security impact. 2. Technology: 3. In-House Technologies:    * 1. Git:  * Manages code versions and changes. * Supports merge/pull request workflows.   + 1. Automated Testing:        - Validates changes via automated unit and integration tests.        - Ensures change does not impact existing functionality.   b. Vendor Technologies:   * + 1. Ticketing Systems (JIRA): * Manages change requests and approval workflow.   + 1. Compliance Scanning Tools: * Ensures changes meet compliance standards. * Automates compliance checks against each change. |
| **Part c** | **Implementation of Approved Changes**   1. Personnel:    1. DevOps Engineers:       1. Apply approved changes via automated pipelines.       2. Monitor the deployment process and handle any deployment issues.    2. Quality Assurance (QA) Team:       1. Conducts thorough testing of changes in pre-production environments.       2. Verifies that changes meet the specified requirements. 2. Technology:    1. In-House Technologies:       1. Continuous Integration/Continuous Deployment (CI/CD) Tools:       2. Jenkins or GitHub Actions to automate the deployment process.    2. Vendor Technologies:       1. Cloud Services ( AWS CloudFormation ):       2. Automate infrastructure setup and changes.       3. Roll back changes automatically if deployment fails   Developers document change justifications in version control systems like Git and collaborate on peer reviews. The Change Management Board oversees these changes, ensuring they are significant and secure. Concurrently, in-house automated testing validates the functionality, and integrated vendor tools like JIRA orchestrate change workflows and compliance checks to maintain standards adherence. |
| **Part d** | **Documentation of Changes and Security Impacts**   1. Personnel:    1. Security Analysts:       1. Assess the security impact of each change.       2. Document the risk analysis and mitigation steps.    2. Compliance Officers:       1. Ensure changes are documented in line with regulatory requirements.       2. Archive all approval records and related communications. 2. Technology:    1. In-House Technologies:       1. Documentation Platforms:       2. Wiki tools like Confluence for maintaining comprehensive change logs.       3. Integration with change management systems to link risk assessments with change documentation.   Security Analysts evaluate and document the security impacts of changes, using tools like Confluence for maintaining logs. Compliance Officers oversee regulatory documentation and archive records. |
| **Part e** | **Tracking Security Flaws and Resolution Reporting**   1. Personnal:    1. Security Operations Team:       1. Monitors and identifies security flaws using tracking systems.       2. Coordinates with IT to ensure timely resolution of identified flaws.    2. Compliance and Reporting Staff:       1. Prepares and delivers reports on flaw resolution status to designated personnel, including FedRAMP officials as required. 2. Technology:    1. In-House Technologies:       1. Systems like JIRA for recording and monitoring security flaws.       2. Automated alerting mechanisms to notify relevant personnel of new and outstanding security issues.       3. Integration with issue tracking systems to ensure all detected flaws are logged and tracked until resolution.   The Security Operations Team utilizes systems like JIRA to monitor and remediate security flaws, with automated alerts for incident tracking. Compliance staff report flaw resolutions to FedRAMP officials. All activities are logged and monitored until resolution. |
|  |  |

#### 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: Chief Technology Officer (CTO) / Lead Software Developer | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate   * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-10 (1) What is the solution and how is it implemented?** |
| --- |
| 1. Personnel:    1. Software Developers are responsible for incorporating integrity checks.       1. Quality Assurance (QA) team ensures the implementation of integrity checks in the CI/CD pipeline. 2. Technology:    1. In-House Technologies:       1. Use of Git commit signing for change integrity.       2. Incorporation of checksums and cryptographic hashes in the build process.       3. Implementation of automated testing to verify integrity during the CI/CD pipeline.    2. Vendor Technologies:       1. Deployment of third-party code signing certificates to ensure software authenticity.       2. Utilizing external integrity verification services (like code signing services).       3. Integration of vendor-provided security scanners to detect and prevent integrity violations. |

### 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: | |
| Parameter SA-11(b)-1: | |
| Parameter SA-11(b)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-11 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-11 (1) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-11 (2) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SA-11 (8) What is the solution and how is it implemented?** |
| --- |
|  |

## System and Communications Protection (SC)

### SC-1 System and Communications Protection Policy and Procedures (L) (M)

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 every three (3) years*]; and
   2. System and communications protection procedures [*FedRAMP Assignment: at least annually*].

| **SC-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter SC-1(a): | |
| Parameter SC-1(b)(1): | |
| Parameter SC-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **SC-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-2 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-4 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter SC-5-1: | |
| Parameter SC-5-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-5 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter SC-6-1: | |
| Parameter SC-6-2: | |
| Parameter SC-6-3: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-6 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter SC-7(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-7 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-7 (3) What is the solution and how is it implemented?** |
| --- |
|  |

#### SC-7 (4) Control Enhancement (M)

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 at least annually*] and removes exceptions that are no longer supported by an explicit mission/business need.

| **SC-7 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter SC-7(4)(e): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-7 (4) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-7 (5) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-7 (7) What is the solution and how is it implemented?** |
| --- |
|  |

#### SC-7 (8) Control Enhancement (M) (H)

The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers at managed interfaces.

| **SC-7 (8)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter SC-7(8)-1: | |
| Parameter SC-7(8)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-7 (8) What is the solution and how is it implemented?** |
| --- |
|  |

#### SC-7 (12) Control Enhancement (M)

The organization implements [*Assignment: organization-defined host-based boundary protection mechanisms*] at [*Assignment: organization-defined information system components*].

| **SC-7 (12)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter SC-7(12)-1: | |
| Parameter SC-7(12)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-7 (12) What is the solution and how is it implemented?** |
| --- |
|  |

#### SC-7 (13) Control Enhancement (M)

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 isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

| **SC-7 (13)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter SC-7(13): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-7 (13) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-7 (18) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter SC-8: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-8 What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter SC-8 (1)-1: | |
| Parameter SC-8 (1)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-8 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### SC-10 Network Disconnect (M)

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 thirty (30) minutes for RAS-based sessions and no longer than sixty (60) minutes for non-interactive user sessions*] of inactivity.

| **SC-10** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter SC-10: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-10 What is the solution and how is it implemented?** |
| --- |
|  |

### 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 Additional FedRAMP Requirements and Guidance:**

**Guidance:** Federally approved and validated cryptography.

| **SC-12** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Cryptographic Key Management Team | |
| Parameter SC-12: Key Management | |
| Implementation Status (check all that apply):  ✅Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ✅ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-12 What is the solution and how is it implemented?** |
| --- |
| Personnel   1. Cryptographic Key Mangement team is responsible for establishing and managing for cryptographic keys   Technology   1. Utilizing AWS key management service for key distribution within AWS environment 2. Using AWS Identify and Access Management for role-based access control to regulate key access. 3. Generating cryptographic keys with approved algorithms.   Detailed Implementation -  We ensured that keys are federally approved and validated cryptographic standards. This involved establishing clear procedures for key generation, distribution, storage , access and destruction. In our organization we used approved cryptographic algorithms and AWS key management service to assist in distribution during the keys generation process. Access to these keys was provided to employees based on their roles, and this is managed by AWS identity and access management . When the keys are no longer required then we destruct the keys and we followed the standard process for doing destruction. Moreover, a detailed documentation maintained to provide a reference for future use by the team . |

#### 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: Cryptographic Key Management Team | |
| Parameter SC-12 (2): Key Management Security | |
| Implementation Status (check all that apply):  ✅ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ✅ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-12 (2) What is the solution and how is it implemented?** |
| --- |
| Personnel -   1. Cryptographic Key Management Team is responsible for key related activities in our orgamization.     Technology -   1. Utilizing NIST-FIPS-compliant key management aligning with AWS 2. Utilizing AWS key management service for secure key stotage 3. Using AWS Identify and Access Management for role-based access control to regulate key access.   Detailed Implementation -  In our organization we follow the NIST FIPS standards to create cryptographic keys . Within our AWS system, we have established clear procedures for managing and sharing these keys. We carefully monitored who can use the keys by closely managing access rights and permissions using AWS Identity and Access Management . We  also use AWS Key Management Service to keep these keys safely stored and making sure they are not accessible to unauthorized individuals . Whenever we use tools outside organization we make sure that they also meet the NISP FIPS standards and integrate smoothly into our AWS setup. |

#### 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: Cryptographic Key Management Team | |
| Parameter SC-12 (3): Key Management Security | |
| Implementation Status (check all that apply):  ✅ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ✅ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-12 (3) What is the solution and how is it implemented?** |
| --- |
| Personnel   1. Cryptographic Key Mangement team is responsible for establishing and managing for cryptographic keys   Technology   1. Utilizing NSA -approved key management technology and process 2. Utilizing AWS key management service for key distribution 3. Using AWS Identify and Access Management for access control 4. Implement hardware security tokens for private key protection 5. Maintain a compliant PKI for approved certificates   Detailed Implementation -  In our organization we have a system for producing , controlling and distributing asymmetric cryptographic keys . We have a team dedicating to manage these keys and they are well trained in the use of NSA-approved key management technology and processes. We followed detailed procedure for key control and distribution which ensure security within our AWS backend . We also use a tool called AWS Identity and Access Management to monitore who can have access to the keys . We have also implemented hardware security tokens to protect user’s private keys in accordance with authorized PKI Class 3 or Class 4 certifications. Also we have maintained a fully compliant Public Key infrastructure to issue authorized certificates . |

### 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: | |
| Parameter SC-13: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-13 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter SC-15(a): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-15 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

**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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-15 What is the solution and how is it implemented?** | |
| --- | --- |
| **Req. 1** |  |

### 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: | |
| Parameter SC-17: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-17 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-18 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-19 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-20 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-21 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-22 What is the solution and how is it implemented?** |
| --- |
|  |

### SC-23 Session Authenticity (M) (H)

The information system protects the authenticity of communications sessions.

| **SC-23** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-23 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter SC-28-1: | |
| Parameter SC-28-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-28 What is the solution and how is it implemented?** |
| --- |
|  |

#### SC-28 (1) Control Enhancement (M)

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*Assignment: organization-defined information system components*]

| **SC-28 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter SC-28(1)-1: | |
| Parameter SC-28(1)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-28 (1) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SC-39 What is the solution and how is it implemented?** |
| --- |
|  |

## System and Information Integrity (SI)

### SI-1 System and Information Integrity Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A system and information integrity 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 information integrity policy and associated system and information integrity controls; and
2. Reviews and updates the current:
   1. System and information integrity policy [*FedRAMP Assignment: at least every three (3) years*]; and
   2. System and information integrity procedures [*FedRAMP Assignment: at least at least annually*].

| **SI-1** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Parameter SI-1(a): | |
| Parameter SI-1(b)(1): | |
| Parameter SI-1(b)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| **SI-1 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: System Administrator | |
| Parameter SI-2(c): | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-2 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | 1. **Personnel**: This responsibility typically falls on IT and security personnel, including system administrators and security analysts. They are responsible for regularly monitoring the system, conducting vulnerability assessments, and identifying security flaws.  2. **Technology**: Vulnerability scanning tools and intrusion detection systems are used to identify flaws. AWS services such as AWS CloudWatch, Inspector, and Trusted Advisor, along with security best practices to automate the identification and reporting of system vulnerabilities. Additionally, ticketing and incident management systems are utilized for tracking and resolving identified flaws. These technologies help automate the process of identifying and reporting system vulnerabilities. Additionally, ticketing and incident management systems are used to report and track identified flaws for resolution. |
| **Part b** | 1. **Personnel**: System administrators, application developers, and quality assurance teams are responsible for testing updates. They ensure that software and firmware updates do not introduce new vulnerabilities or disrupt system functionality.  2. **Technology**: Test environments are set up to simulate the production environment. Automated testing tools and scripts may be used to check for side effects and verify the effectiveness of updates. Automated testing tools and scripts play a pivotal role in this process. AWS Lambda, for instance, can be employed to automate testing procedures, run test cases, and trigger specific actions based on the outcomes. Amazon CloudWatch can be configured to monitor the performance and behavior of the test environments, generating alarms in case of anomalies, thereby providing an additional layer of validation. Moreover, AWS Step Functions can orchestrate the testing workflow, allowing for the creation of complex, multi-step tests that assess the effectiveness of updates comprehensively.  Change management systems help in tracking and managing the testing process. |
| **Part c** | 1. **Personnel**: System administrators and IT operations teams are responsible for ensuring timely installation of security updates. Compliance personnel ensure that updates are installed within the required timeframe.  2. **Technology**: Patch management tools are used to automate the distribution and installation of updates. AWS Systems Manager can be accessed through the AWS Management Console, and organizations can define their patching policies, schedules, and targets, which specify the AWS instances to be patched. Once set up, AWS Systems Manager automates the patch management process, making it easier to maintain system integrity and meet compliance requirements. These tools can schedule and deploy updates to meet the FedRAMP requirement of installing security updates within 30 days of release. |
| **Part d** | 1.**Personnel**: Configuration management teams, IT governance, and compliance officers play a key role in incorporating flaw remediation into the organizational configuration management process. They ensure that the configuration management process includes the identification and remediation of security flaws.  2.**Technology**: Configuration management tools, version control systems, and change management systems are used to document and track changes related to flaw remediation. AWS Config enables continuous monitoring and assessment of AWS resource configurations, making it an ideal tool for documenting and tracking changes. It provides a historical record of resource configurations and offers automated notifications when changes occur. This ensures that any changes related to flaw remediation are well-documented and can be reviewed for compliance. These tools ensure that flaw remediation is integrated into the larger organizational configuration management process. |

#### 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: IT Admin | |
| Parameter SI-2 (2): | |
| Implementation Status (check all that apply):  ✓ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-2 (2) What is the solution and how is it implemented?** |
| --- |
| **1.Personnel**: In the context of implementing automated mechanisms to determine the state of information system components with regard to flaw remediation, personnel primarily focus on the initial setup, configuration, and monitoring of these automated tools and processes. IT and security personnel, including system administrators and security analysts, play a pivotal role in configuring and managing the automated vulnerability assessment and scanning tools.  **2.Technology**: The technology aspect involves the utilization of automated tools and systems for vulnerability scanning and flaw remediation assessment. sentinel shield also employ intrusion detection systems (IDS) to further monitor and detect any emerging security issues. In the AWS context, AWS Config, AWS Inspector, and AWS Security Hub can be integrated to automate the scanning and assessment process. These AWS services can be configured to regularly scan and assess the state of AWS resources, providing automated reports on security flaws and vulnerabilities. By leveraging AWS technologies, organizations can ensure that automated mechanisms are in place to assess the state of information system components on a monthly basis, helping to maintain security and compliance in their cloud environments. |

#### 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: Security Operations Admin (COA) and Chief Information Security Officer (CISO) | |
| Parameter SI-2(3)(b): The organization should define specific benchmarks for taking corrective actions. These benchmarks may include criteria related to security posture, compliance with security policies, response timeframes, and other relevant factors. | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-2 (3) What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | Personnel:   1. The organization designates specific personnel responsible for measuring the time between flaw identification and flaw remediation. 2. These designated personnel possess the skills and knowledge required to effectively track, analyze, and reduce the time taken to address identified security flaws. 3. Personnel responsible for this task have a strong understanding of security vulnerabilities, remediation processes, and the AWS environment.   Technology:  The application leverages several Amazon Web Services (AWS) technologies and other tools to facilitate the measurement of the time between flaw identification and flaw remediation. Key technologies and tools relevant to this control enhancement include:   1. AWS CloudTrail: Records API calls and actions taken on AWS resources, helping to trace and analyze security events and flaw remediation activities. 2. AWS Config: Provides configuration history and compliance monitoring, enabling the tracking of changes made to AWS resources and their impact on security. 3. AWS CloudWatch: Offers monitoring, alarms, and dashboards to track the performance of AWS resources and the response to security incidents. 4. Security Information and Event Management (SIEM) tools: Third-party SIEM solutions can be integrated to centralize log and event data for analysis and reporting.   Detailed Implementation:  The organization implements a comprehensive approach to measure the time between flaw identification and flaw remediation. This approach involves the following steps:   1. Flaw Identification: When security flaws are identified, designated personnel record and document the details of the flaw, including its nature, severity, and potential impact. 2. Flaw Tracking: Using AWS CloudTrail, AWS Config, and other relevant tools, the organization tracks the timeline of the flaw from identification to resolution. This includes recording the exact date and time of flaw detection. 3. Remediation Planning: Personnel analyze the nature of the flaw and initiate remediation planning, which may involve creating a task list, assigning responsibilities, and setting priorities. 4. Timely Remediation: The organization actively works to remediate identified security flaws, ensuring that the remediation process is carried out within a reasonable and predefined timeframe. 5. Continuous Monitoring: AWS CloudWatch and other monitoring tools are used to continuously assess the progress of flaw remediation and to trigger alerts if remediation takes longer than expected. 6. Documentation: Detailed records are maintained for each flaw, including the time taken for identification and remediation, the actions taken, and any lessons learned during the process. 7. Analysis and Improvement: The organization regularly reviews the data on flaw identification and remediation timeframes to identify trends and areas for improvement, with the goal of reducing the time taken to remediate flaws. |
| **Part b** | Personnel:   1. The organization designates specific personnel responsible for establishing organization-defined benchmarks for taking corrective actions. 2. These designated personnel possess the skills and knowledge required to define appropriate benchmarks and understand the specific security requirements of the AWS environment. 3. Personnel responsible for this task have a strong understanding of security best practices and the AWS services being utilized.   Technology:  The project application leverages various Amazon Web Services (AWS) technologies to support its operations and facilitate the establishment of benchmarks for taking corrective actions. Key AWS technologies relevant to this control enhancement include:   1. AWS Config: Provides configuration history and compliance monitoring, enabling the organization to track changes made to AWS resources and evaluate their adherence to established benchmarks. 2. AWS CloudWatch: Offers monitoring, alarms, and dashboards to track the performance of AWS resources and the organization's progress in achieving corrective actions based on the defined benchmarks.   Detailed Implementation:  The organization implements a structured approach to establish organization-defined benchmarks for taking corrective actions. This approach encompasses the following steps:   1. Benchmark Definition: Designated personnel work in collaboration with relevant stakeholders to define organization-specific benchmarks for corrective actions. These benchmarks are established based on recognized security best practices, regulatory requirements, and the specific security needs of the project. 2. Benchmark Documentation: The established benchmarks are documented clearly, outlining the criteria, timelines, and objectives for corrective actions. This documentation serves as a reference for measuring the effectiveness of security improvements. 3. Benchmark Alignment: The organization aligns its security policies and procedures with the defined benchmarks, ensuring that corrective actions are consistent with these established goals. 4. Monitoring and Compliance: AWS Config is used to continuously monitor the configuration of AWS resources, while AWS CloudWatch tracks the organization's performance in relation to the defined benchmarks. Alerts and notifications are configured to trigger corrective actions when deviations occur. 5. Corrective Action Plans: When deviations from the established benchmarks are identified, the organization formulates corrective action plans to address the specific issues and bring the systems into compliance. 6. Performance Evaluation: Regular reviews are conducted to evaluate the effectiveness of corrective actions in achieving the defined benchmarks. Adjustments and improvements are made as needed. 7. Documentation and Reporting: Comprehensive records are maintained for all corrective actions taken in response to benchmark deviations, including the actions, outcomes, and any lessons learned. 8. Continuous Improvement: The organization continually refines the established benchmarks and associated corrective actions based on evolving threats, technological advancements, and changes in security requirements. |

### SI-3 Malicious Code Protection (L) (M)

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 alerting administrator or defined security personnel*] 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: | |
| Parameter SI-3(c)(1)-1: | |
| Parameter SI-3(c)(1)-2: | |
| Parameter SI-3(c)(2): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-3 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | Personnel:   1. Security Team: The security team is responsible for researching and implementing effective malicious code protection mechanisms at system entry and exit points. 2. Incident Response Team: The incident response team is responsible for monitoring and responding to any security alerts related to malicious code. 3. System Administrators: System administrators are responsible for configuring and maintaining the technology solutions designed to detect and eradicate malicious code.   Technology:   1. Malicious Code Protection Technology    1. The organization employs intrusion detection systems (IDS), intrusion prevention systems (IPS), and advanced antivirus solutions at entry and exit points of the information system to detect and eradicate malicious code.    2. These technologies are configured to perform real-time scans of incoming and outgoing traffic and to block or quarantine any detected malicious code. 2. Regular Updates and Maintenance    1. The organization ensures that malicious code protection mechanisms are kept up-to-date with the latest threat intelligence, virus definitions, and security patches.    2. Regular maintenance and monitoring of these technologies are conducted to maintain their effectiveness.   Detailed Implementation:   1. Malicious Code Detection    1. Malicious code protection mechanisms are implemented at both the entry and exit points of the information system, including firewalls, email gateways, and web application firewalls.    2. These mechanisms are configured to scan all incoming and outgoing data for signs of malicious code, such as viruses, malware, and other threats. 2. Eradication Procedures    1. When malicious code is detected, automated procedures are triggered to eradicate the threat. This may involve isolating, quarantining, or removing the affected files or data.    2. The incident response team is alerted to investigate and initiate further actions as necessary. |
| **Part b** | Personnel:   1. Security Team: The security team is responsible for monitoring and identifying new releases and updates for malicious code protection mechanisms. 2. Configuration Management Team: The configuration management team is responsible for defining and implementing policies and procedures for updating security mechanisms. 3. System Administrators: System administrators are responsible for executing the updates and ensuring that they do not disrupt the operational environment.   Technology:   1. Update Mechanisms    1. The organization utilizes automated update mechanisms to receive new releases and updates for malicious code protection mechanisms, such as antivirus software and intrusion detection systems.    2. These update mechanisms are configured to ensure timely receipt of the latest security definitions and patches. 2. Compatibility Testing    1. Before applying updates, the organization conducts compatibility testing to ensure that the updates do not negatively impact system functionality and performance.    2. Testing is performed in a controlled environment to mitigate risks associated with updates.   Detailed Implementation:   1. Update Monitoring    1. The security team continuously monitors sources of information, such as vendor notifications and threat intelligence feeds, for new releases and updates for malicious code protection mechanisms.    2. Notifications are promptly relayed to the configuration management team for review. 2. Configuration Management Procedures    1. Configuration management procedures are defined and documented. These procedures include guidelines for assessing the impact of updates and scheduling maintenance windows.    2. The procedures also detail how to back up existing configurations and apply updates while adhering to change management protocols. 3. Update Validation    1. After updates are applied, the system administrators validate their successful implementation and verify that the malicious code protection mechanisms are operating effectively.    2. This validation ensures that the organization is adequately protected against the latest threats. |
| **Part c** | Personnel:   1. Security Team: The security team is responsible for configuring and maintaining the malicious code protection mechanisms, including defining scanning schedules and alerting criteria. 2. System Administrators: System administrators play a crucial role in implementing the configurations as defined by the security team. 3. Alerting Administrator/Defined Security Personnel: Identified personnel are responsible for responding to alerts generated by malicious code detection and initiating appropriate remediation actions.   Technology:   1. Periodic Scans    1. The organization configures malicious code protection mechanisms, such as antivirus software and intrusion detection systems, to perform periodic scans of the entire information system at least weekly. These scans check the system for signs of malicious code. 2. Real-Time Scans    1. Real-time scans are configured to be performed on files from external sources, including endpoints, as the files are downloaded, opened, or executed. This ensures that any malicious code is detected and addressed in real-time. 3. Alerting Mechanisms    1. Alerting mechanisms are integrated into malicious code protection mechanisms to alert either the system administrator or defined security personnel when malicious code is detected.    2. Alerts are configured to provide information on the nature of the threat and the location of the affected files.   Detailed Implementation:   1. Configuration of Periodic Scans    1. The security team defines the schedule for periodic scans, ensuring that they are conducted at least weekly.    2. Scans are configured to analyze the entire information system, including all critical endpoints. 2. Configuration of Real-Time Scans    1. Real-time scanning mechanisms are configured to scan files from external sources, including files downloaded from the internet, email attachments, and files opened or executed on endpoints.    2. Real-time scans are configured to detect and prevent the execution of files with malicious code. 3. Alerting Procedures    1. The security team defines alerting criteria and procedures for responding to malicious code detection.    2. When malicious code is detected, alerts are generated and sent to the designated administrator or security personnel.    3. Clear guidelines for responding to alerts, including isolation, quarantine, and remediation procedures, are documented. |
| **Part d** | Personnel:   1. Security Team: The security team is responsible for monitoring and assessing alerts generated by malicious code detection mechanisms, including identifying and addressing false positives. 2. Incident Response Team: The incident response team is responsible for verifying and mitigating the potential impact of false positives on the availability of the information system.   Technology:   1. False Positive Handling Technology    1. The organization employs technology solutions, such as advanced antivirus software, that are designed to minimize false positives during malicious code detection.    2. False positive handling technology is integrated into the security infrastructure to reduce the impact on system availability. 2. Alert Validation Mechanisms    1. Alert validation mechanisms are implemented to assess the validity of alerts generated by malicious code detection mechanisms.    2. These mechanisms use heuristics, behavioral analysis, and threat intelligence to distinguish between false positives and actual threats.   Detailed Implementation:   1. False Positive Review Process    1. The security team establishes a procedure for reviewing and validating alerts that may be false positives. This includes examining the source of the alert and assessing its potential impact on system availability.    2. False positives are documented, and measures are taken to avoid repeating the same false positive detection in the future. 2. Impact Assessment    1. In the event of a false positive alert that could impact system availability, the incident response team assesses the potential consequences.    2. If necessary, temporary mitigations or adjustments are applied to maintain system availability while preserving security. 3. Continuous Improvement    1. The organization maintains a continuous improvement process to refine malicious code detection mechanisms, reducing the occurrence of false positives.    2. Lessons learned from previous incidents are used to enhance the organization's overall security posture. |

#### SI-3 (1) Control Enhancement (M) (H)

The organization centrally manages malicious code protection mechanisms.

| **SI-3 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-3 (1) What is the solution and how is it implemented?** |
| --- |
| Personnel:  Technology:  Detailed 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-3 (2) What is the solution and how is it implemented?** |
| --- |
| Personnel:  Technology:  Detailed Implementation: |

#### SI-3 (7) Control Enhancement (M) (H)

The information system implements nonsignature-based malicious code detection mechanisms.

| **SI-3 (7)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-3 (7) What is the solution and how is it implemented?** |
| --- |
| Personnel:  Technology:  Detailed 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: | |
| Parameter SI-4(a)(1): | |
| Parameter SI-4(b): | |
| Parameter SI-4(g)-1: | |
| Parameter SI-4(g)-2: | |
| Parameter SI-4(g)-3: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-4 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |
| **Part e** |  |
| **Part f** |  |
| **Part g** |  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-4 (1) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-4 (2) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter SI-4(4): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-4 (4) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter SI-4(5)-1: | |
| Parameter SI-4(5)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-4 (5) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-4 (14) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-4 (16) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter SI-4(23)-1: | |
| Parameter SI-4(23)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-4 (23) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: Security Operations Center (SOC) and Chief Information Security Officer (CISO) | |
| Parameter SI-5(a): Ensure that the SOC has established continuous monitoring and communication mechanisms such as US-CERT to promptly receive relevant security alerts and advisories. | |
| Parameter SI-5(c): Ensure that the Communication and Notification Team is equipped with secure communication channels and processes for the timely and targeted dissemination of security information. | |
| Implementation Status (check all that apply):   * ~~Implemented~~   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (with security directives.  Detailed Implementation:  The organization implements a comprehensive approach to implement security directives and manage noncompliance in accordance with established timeframes. This approach includes the following steps:   1. Directive Review: Designated personnel regularly review security directives received from the issuing organization and assess their applicability to the application. 2. Compliance Assessment: Using AWS Config, the organization continuously monitors the configuration of AWS resources to evaluate their compliance with established security directives. 3. Timely Implementation: Personnel ensure that security directives are implemented within the established timeframes. This may involve making configuration changes, applying patches, or updating security settings as necessary. 4. Automated Checks: AWS CloudWatch Events and AWS Lambda can be utilized to automate compliance checks and responses to noncompliance, ensuring timely remediation. 5. Noncompliance Notification: In cases where full compliance cannot be achieved within the established timeframes, the organization notifies the issuing organization of the degree of noncompliance and any mitigating actions being taken. 6. Record Keeping: Detailed records are maintained regarding the implementation of security directives, including compliance status, actions taken, and communication with the issuing organization.   Continuous Improvement: The organization periodically reviews its processes for implementing security directives to enhance efficiency and effectiveness.Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-5 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | Personnel:   1. The organization designates specific personnel responsible for monitoring and receiving information system security alerts, advisories, and directives. 2. These designated personnel have the necessary skills and training to understand and act upon the information received from sources such as US-CERT. 3. The organization ensures that personnel are familiar with the procedures for responding to malicious code alerts and advisories.   Technology:  The project leverages a range of Amazon Web Services (AWS) technologies to support its operations. Some of the key AWS technologies utilized in the context of malicious code protection include:   1. Amazon GuardDuty: An AWS managed threat detection service that continuously monitors for malicious activity and unauthorized behavior within the AWS environment. 2. AWS WAF (Web Application Firewall): Provides protection against web application attacks, including SQL injection, cross-site scripting (XSS), and other common security threats. 3. Amazon Inspector: An automated security assessment service that helps identify vulnerabilities and deviations from best practices in your applications.   Detailed Implementation:  The organization implements a comprehensive approach to malicious code protection, which includes the following steps:   1. Continuous Monitoring: Personnel responsible for monitoring and receiving security alerts regularly access information system security alerts, advisories, and directives from US-CERT. This monitoring is performed on an ongoing basis to ensure timely awareness of potential threats and vulnerabilities. 2. Alert Triage: When a security alert or advisory is received, designated personnel promptly review and triage the information to determine its relevance and potential impact on the application. 3. Response Planning: In the event that a malicious code or security threat is identified, the organization has established response procedures to contain and mitigate the threat. This includes isolating affected systems, applying security patches, and notifying relevant stakeholders. 4. Patch Management: The organization maintains a patch management process to ensure that the AWS infrastructure, including the aforementioned technologies, is kept up-to-date with the latest security updates and patches. 5. Regular Training: Personnel involved in the monitoring and response to security alerts receive regular training to enhance their skills and knowledge in identifying and responding to malicious code and security threats. 6. Reporting and Documentation: All actions taken in response to security alerts, advisories, and directives are documented for audit and compliance purposes. This includes documenting the steps taken to address identified threats and vulnerabilities. 7. Ongoing Improvement: The organization regularly reviews and updates its malicious code protection measures to adapt to evolving threats and security best practices. |
| **Part b** | Personnel:   1. The organization designates specific personnel responsible for generating internal security alerts, advisories, and directives when deemed necessary. 2. These designated personnel possess the expertise and knowledge required to identify, assess, and respond to potential security threats within the AWS environment. 3. Personnel are trained in incident detection, response, and reporting procedures, ensuring they can effectively generate and communicate internal security alerts, advisories, and directives.   Technology:  The application relies on various Amazon Web Services (AWS) technologies to facilitate its operations. Key AWS technologies relevant to generating and responding to internal security alerts, advisories, and directives include:   1. Amazon CloudWatch: Provides real-time monitoring and operational insights into the AWS resources and applications, allowing for the creation of custom alarms and notifications based on specific security events and thresholds. 2. Amazon SNS (Simple Notification Service): Enables the distribution of messages and alerts to various endpoints, including email, SMS, and application endpoints, allowing for rapid dissemination of security alerts and advisories to relevant stakeholders. 3. AWS Lambda: Can be used to automate the execution of actions in response to security alerts, including triggering specific incident response procedures.   Detailed Implementation:  The organization implements a comprehensive approach to generating and disseminating internal security alerts, advisories, and directives, encompassing the following steps:   1. Threat Detection: Using AWS technologies like Amazon CloudWatch, the organization continuously monitors the AWS environment for signs of malicious code, unauthorized access, or other security anomalies. 2. Incident Identification: When potential security threats are detected, designated personnel promptly investigate and assess the situation to determine if it warrants the generation of internal security alerts. 3. Alert Criteria: The organization establishes predefined criteria for determining when an internal security alert or advisory should be generated. These criteria are based on known threat indicators, unusual activity patterns, or other security-related anomalies. 4. Alert Generation: If the predefined criteria are met, designated personnel generate internal security alerts or advisories that provide details about the threat, its potential impact, and recommended actions for mitigation. 5. Stakeholder Notification: Security alerts and advisories are distributed to relevant stakeholders using Amazon SNS, ensuring that the right personnel are promptly informed about the security incident. 6. Incident Response: In response to internal security alerts, the organization follows predefined incident response procedures, including isolating affected systems, applying security patches, and taking necessary steps to mitigate the threat. 7. Documentation and Reporting: All actions taken, from alert generation to incident response, are documented for audit and compliance purposes. This documentation includes a record of the security incident, the actions taken, and lessons learned for continuous improvement. 8. Ongoing Refinement: The organization periodically reviews and updates its internal security alert and advisory procedures to adapt to emerging threats and ensure that the AWS infrastructure remains protected. |
| **Part c** | Personnel:   1. The organization designates specific personnel responsible for disseminating security alerts, advisories, and directives to relevant stakeholders. These personnel have the necessary expertise and training to understand and communicate security-related information effectively. 2. System security personnel, including Security Administrators and Administrators with configuration/patch-management responsibilities, are identified as key recipients of security alerts. 3. The organization ensures that designated personnel are well-versed in security best practices, incident response procedures, and the specific responsibilities associated with their roles.   Technology:  The application leverages a suite of Amazon Web Services (AWS) technologies to support its operations and facilitate the dissemination of security alerts, advisories, and directives to stakeholders. Key AWS technologies relevant to this control include:   1. Amazon SNS (Simple Notification Service): Used to distribute messages and alerts to the specified recipients, such as system security personnel and administrators. It supports various communication channels, including email, SMS, and application endpoints. 2. AWS Lambda: Can be employed to automate the process of disseminating alerts and advisories by triggering predefined actions based on specific events or criteria. 3. AWS IAM (Identity and Access Management): Ensures that access to AWS resources and services is appropriately controlled and managed, safeguarding the dissemination process.   Detailed Implementation:  The organization implements a robust approach to disseminating security alerts, advisories, and directives to relevant stakeholders, including system security personnel and administrators with configuration/patch-management responsibilities. This approach encompasses the following steps:   1. Alert Generation: When security alerts are received or generated internally, designated personnel assess their relevance and potential impact. 2. Recipient Identification: The organization maintains an up-to-date list of recipients, including system security personnel and administrators responsible for configuration and patch management. This list is periodically reviewed and updated. 3. Alert Categorization: The organization categorizes security alerts based on their severity and relevance to the specific roles of the recipients, ensuring that information is appropriately targeted. 4. Alert Dissemination: Using Amazon SNS, the organization sends security alerts, advisories, and directives to the identified recipients through their preferred communication channels. 5. Automated Actions: AWS Lambda can be utilized to automate predefined actions based on specific alerts, such as initiating patch management or isolation procedures. 6. Access Control: AWS IAM is used to control access to the systems and services involved in the dissemination process, ensuring that only authorized personnel can send, receive, or act upon security alerts. 7. Confirmation and Acknowledgment: The organization may establish confirmation and acknowledgment procedures to verify that recipients have received and understood the security information. 8. Documentation: All security alerts, advisories, and directives are documented, including details about the dissemination process, recipients, and responses. 9. Continuous Improvement: The organization periodically reviews its security alert dissemination procedures to enhance their effectiveness and adapt to emerging threats. |
| **Part d** | Personnel:   1. The organization designates specific personnel responsible for implementing security directives in accordance with established timeframes or for notifying the issuing organization of the degree of noncompliance. 2. These designated personnel have the necessary knowledge and authority to ensure timely compliance with security directives and to communicate effectively with the issuing organization. 3. Personnel responsible for compliance are well-versed in security policies, procedures, and the specific requirements outlined in the security directives.   Technology:  The application relies on a variety of Amazon Web Services (AWS) technologies that support the implementation and monitoring of security directives. Key AWS technologies relevant to this control include:   1. AWS Config: Allows for the assessment, tracking, and compliance monitoring of AWS resource configurations. It provides insights into resource changes and their adherence to established security policies. 2. AWS CloudWatch Events: Provides automated event response capabilities, which can be used to trigger actions in response to noncompliance with security directives. 3. AWS Lambda: Can be employed to automate compliance checks and actions in response to noncompliance |

### 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: | |
| Parameter SI-6(a): | |
| Parameter SI-6(b): | |
| Parameter SI-6(c): | |
| Parameter SI-6(d)-1: | |
| Parameter SI-6(d)-2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-6 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |
| **Part c** |  |
| **Part d** |  |

### 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: | |
| Parameter SI-7: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-7 What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter SI-7(1)-1: | |
| Parameter SI-7(1)-2: | |
| Parameter SI-7(1)-3: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-7 (1) What is the solution and how is it implemented?** |
| --- |
|  |

#### 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: | |
| Parameter SI-7 (7): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-7 (7) What is the solution and how is it implemented?** |
| --- |
|  |

### 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: CSO(Chief Security Officer) & Security Engineering Lead | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific   * Service Provider Hybrid (Corporate and System Specific)   ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-8 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** | Spam protection is deployed by both the CSO (Chief Security Officer) and the Security Engineering Lead and done through AWS (Amazon Web Services). We use Amazon WorkMail as our email client since it allows us to create security proxies and gateways for our email client. Using WorkMail and AWS allows us to create extensive spam filters based on machine learning models that we can train ourselves (with our own and external data) and use it as a gateway between incoming and outgoing mail. This system can detect if incoming mail is spam as well as we set up rules to immediately delete spam and report it if it contains some sort of suspicious file or text (e.g., .exe, .sh, http link(s), etc.). |
| **Part b** | Our spam protection system is regularly monitored and updated. This system is monitored 24/7 and our email client is updated directly by AWS (since it’s cloud-based). Our training models to detect spam are updated every month. We do remove spam from email clients immediately, but we do collect logs of such emails caught as spam to be able to keep training our model on what spam/phishing looks like. Nowadays, spam and phishing emails are getting a lot more elaborate thanks to AI and verified-looking domain names. We use this data to regularly train our models so that none of our systems are compromised if someone were to open one of these files/links by mistake. |

#### SI-8 (1) Control Enhancement (M) (H)

The organization centrally manages spam protection mechanisms.

| **SI-8 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: CSO(Chief Security Officer) & Security Engineering Lead | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific   * Service Provider Hybrid (Corporate and System Specific)   ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-8 (1) What is the solution and how is it implemented?** |
| --- |
| Our organization's approach to centrally managing spam protection mechanisms is done by the Chief Security Officer (CSO) and the Security Engineering Lead, utilizing the infrastructure provided by AWS. The central management system facilitates the deployment of Amazon WorkMail's security features across the organization, ensuring consistent spam filter policies and rules are applied at all information system entry and exit points. This centralized framework permits real-time adjustments and updates to the spam protection mechanisms, which is critical for adapting to the evolving nature of spam and phishing tactics. Also Centralized logging and reporting through AWS enable the organization to collect and analyze data on detected spam, fine-tuning the machine learning models on a regular basis. The benefit of this arrangement is a robust, scalable spam defense that is maintained in concert with the organization’s broader security posture and cloud-first strategy, ensuring that the system's defenses evolve in lockstep with the latest cyber threats. |

#### SI-8 (2) Control Enhancement (M) (H)

The organization automatically updates spam protection mechanisms.

| **SI-8 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: IT Security Operations Lead | |
| Implementation Status (check all that apply):   * Implemented   ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate   * Service Provider System Specific   ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-8 (2) What is the solution and how is it implemented?** |
| --- |
| Our organization security team ensures that these systems are always operating with the most current and effective detection capabilities. The process is implemented through the use of cloud-based services, which inherently offer the advantage of seamless, automatic updates. The spam protection service, such as Amazon WorkMail mentioned previously, is configured to receive and implement updates as soon as they are released by the provider. This minimizes the window of vulnerability between the emergence of new spam techniques and the deployment of protective measures against them.This automated update process is integrated within the organization's security operations protocols, which includes continuous monitoring of spam filter performance and regular reviews of update logs to verify successful implementation of new updates. The system is set to alert the security team in the event of any issues during the update process. |

### 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: | |
| Parameter SI-10: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-10 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter SI-11(b): | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-11 What is the solution and how is it implemented?** | |
| --- | --- |
| **Part a** |  |
| **Part b** |  |

### 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: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-12 What is the solution and how is it implemented?** |
| --- |
|  |

### 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: | |
| Parameter SI-16-1: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| **SI-16 What is the solution and how is it implemented?** |
| --- |
|  |

# 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

*Instruction: Attach any documents that are referred to in the Information System Name (Enter Information System Abbreviation) System Security Plan. Documents and attachments should, provide the title, version and exact file name, including the file extension. All attachments and associated documents must be delivered separately. No embedded documents will be accepted.*

*Delete this and all other instructions from your final version of this document.*

# Attachments

A recommended attachment file naming convention is <information system abbreviation> <attachment number> <document abbreviation> <version number> (for example, "Information System Abbreviation A8 IRP v1.0"). Use this convention to generate names for the attachments. Enter the appropriate file names and file extensions in Table 15-1 to describe the attachments provided. Make only the following additions/changes to Table 15-1:

* The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15-1. Attachment File Naming Convention to differentiate between them using the “xx” portion of the File Name. *Example* Enter Information System Abbreviation *A1 ISPP xx v1.0*. Delete the “xx” if there is only one document.
* Enter the file extension for each attachment.
* Do not change the Version Number in the File Name in Table 15-1. Attachment File Naming Convention. (Information System Abbreviation, attachment number, document abbreviation, version number)

*Table 15-1. Names of Provided Attachments*

| **Attachment** | **File Name** | **File Extension** |
| --- | --- | --- |
| **Information Security Policies and Procedures** | Enter Information System Abbreviation A1 ISPP xx v1.0 | . enter extension |
| **User Guide** | Enter Information System Abbreviation A2 UG v1.0 | . enter extension |
| **Digital Identity Worksheet** | Included in Section 15 |  |
| **PTA** | Included in Section 15 |  |
| **PIA If needed)** | Enter Information System Abbreviation A4 PIA v1.0 | . enter extension |
| **Rules of Behavior** | Enter Information System Abbreviation A5 ROB v1.0 | . enter extension |
| **Information System Contingency Plan** | Enter Information System Abbreviation A6 ISCP v1.0 | . enter extension |
| **Configuration Management Plan** | Enter Information System Abbreviation A7 CMP v1.0 | . enter extension |
| **Incident Response Plan** | Enter Information System Abbreviation A8 IRP v1.0 | . enter extension |
| **CIS Workbook** | Enter Information System Abbreviation A9 CIS Workbook v1.0 | . enter extension |
| **FIPS 199** | Included in Section 15 |  |
| **Inventory** | Enter Information System Abbreviation A13 INV v1.0 | . enter extension |

1. **Information Security Policies and Procedures**

All Authorization Packages must include an Information Security Policies and Procedures attachment, which will be reviewed for quality.

1. **User Guide**

All Authorization Packages must include a User Guide attachment, which will be reviewed for quality.

1. **Digital Identity Worksheet**

*This Attachment Section has been revised to include the Digital Identity template. Therefore, a separate attachment is not needed. Delete this note and all other instructions from your final version of this document.*

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 the (Enter Information System Abbreviation) in accordance with NIST SP 800-63-3.

*Table 15-2. Information System Name and Title*

| **Unique Identifier** | **Information System Name** | **Information System Abbreviation** |
| --- | --- | --- |
| Enter FedRAMP Application Number. |  | Enter Information System Abbreviation |

### 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

CSP Name has assessed the potential risk from Digital Identity errors, or Digital Identity misuse, related to a user’s asserted identity. CSP Name 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

*Instruction: Select the lowest level that will cover all potential impact identified from Table 15-4 Potential Impacts for Assurance Levels.*

*Delete this instruction from your final version of this document.*

The CSP Name has identified that they support the Digital Identity Level that has been selected for the <Information System Name> 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 | ☐ |

1. **PTA / PIA**

*This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are “Yes” then complete a Privacy Impact Assessment Template and include it as an Attachment.*

*Delete this note and all other instructions from your final version of this document.*

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 - Information System Name; Privacy POC individual is identified as the Information System Name; Privacy Officer and POC for privacy at CSP Name.

*Table 15-6. - Information System Name; Privacy POC*

| **Name** | Click here to enter text. |
| --- | --- |
| **Title** | Click here to enter text. |
| **CSP / Organization** | Click here to enter text. |
| **Address** | Click here to enter text. |
| **Phone Number** | Click here to enter text. |
| **Email Address** | Click here to enter text. |

#### 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 Information System Name Laws and Regulations include additional laws and regulations that are specific to <Information System Name>. 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. <Information System Name> Laws and Regulations*

| **Identification Number** | **Title** | **Date** | **Link** |
| --- | --- | --- | --- |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |

#### 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 Information System Name Standards and Guidance includes any additional standards and guidance that are specific to <Information System Name>. 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. <Information System Name> Standards and Guidance*

| **Identification Number** | **Title** | **Date** | **Link** |
| --- | --- | --- | --- |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |

#### 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

CSP Name performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the <Information System Name> (Enter Information System Abbreviation) components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by CSP Name can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

#### Qualifying Questions

| Select One | Does the ISA collect, maintain, or share PII in any identifiable form? |
| --- | --- |
| Select One | Does the ISA collect, maintain, or share PII information from or about the public? |
| Select One | Has a Privacy Impact Assessment ever been performed for the ISA? |
| Select One | Is there a Privacy Act System of Records Notice (SORN) for this ISA system?  If yes; the SORN identifier and name is: Enter SORN ID/Name. |

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).

1. **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.

1. **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.

1. **Configuration Management Plan**

All Authorization Packages must include a Configuration Management Plan attachment, which will be reviewed for quality.

1. **Incident Response Plan**

All Authorization Packages must include an Incident Response Plan attachment, which will be reviewed for quality.

1. **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).

1. **FIPS 199**

*This Attachment Section has been revised to include the FIPS 199 Template. Therefore, a separate PTA attachment is not needed. Delete this note and all other instructions from your final version of this document.*

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

The <Information System Name> system has been determined to have a security categorization of Choose level.

*Instruction: Insert a brief high-level description of the system, the system environment and the purpose of the system. The description should be consistent with the description found in the System Security Plan (SSP).   
Delete this instruction from your final version of this document.*

### Methodology

*Instruction: The CSP should review the NIST Special Publication 800-60 Volume 2 Revision 1 Appendix C Management and Support Information and Information System Impact Levels and Appendix D Impact Determination for Mission-Based Information and Information Systems to assess the recommended impact level for each of the information types. For more information, the CSP should also consult Appendix D.2. After reviewing the NIST guidance on Information Types, the CSP should fill out Table 2-1 CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1.   
Delete this instruction from your final version of this document.*

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.

*Instruction: In the first three columns, put the NIST SP-60 V2 R1 recommended impact level. In the next three columns, put in the CSP determined recommended impact level. If the CSP determined recommended impact level does not match the level recommended by NIST, put in an explanation in the last column as to why this decision was made.   
Delete this instruction from your final version of this document.*

The Table 2-1 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** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |

1. **Separation of Duties Matrix**

All Authorization Packages have the option to provide a Separation of Duties Matrix attachment, which will be reviewed for quality.

ATTACHMENT 11 - Separation of Duties Matrix is referenced in the following controls.

AC-5 Separation of Duties (M) (H) Additional FedRAMP Requirements and Guidance

1. **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>

1. **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.