**FedRAMP Tailored [System Name] Attestation Statement**

|  |
| --- |
| I, [System Owner Name] am the system owner for [Cloud Service Provider (CSP) Name and System Name]. I attest to the accuracy of the statements in this document. I understand any willful misrepresentation of the information presented here will result in immediate revocation of this system’s authorization to operate.  System Owner’s Signature: X\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  <System Owner’s Name>  <CSP Name> -- <System Name> |

## Attestation of Policies and Procedures

The following policies and procedures exist and address the basic elements listed for this system. The policies are reviewed and updated at least every three years. The procedures are reviewed and updated annually. Exceptions are identified in the *Modifications* column.

Where policies or procedures are fully inherited, simply state, “This is inherited.” in the Modification Statement column. For a fully virtual SaaS this is likely true for PE-1, Physical and Environment Protection Policy and Procedures, and may be true for others.

**Do not delete rows or modify the Basic Elements column in the tables below. State any exceptions in the Modifications Statement column.**

| **No.** | **Control ID** | **Control Name** | **Basic Elements** | **Modification Statement** |
| --- | --- | --- | --- | --- |
| 1. | AC-1 | Access Control Policy and Procedures | * Ensures access to the system is authorized and granted consistently. * Ensures only authorized individuals have administrative access to the system. |  |
| 2. | AT-1 | Security Awareness and Training Policy and Procedures | * Ensures all CSP staff who administer the system receive security awareness training at least annually. * Ensures staff are aware of all relevant policies and procedures. |  |
| 3. | AU-1 | Audit and Accountability Policy and Procedures | * Ensures the system is producing appropriate audit logs. * Ensures the system is retaining audit logs for an appropriate amount of time. * Ensures the audit logs are reviewed periodically, after an incident is identified, and after relevant exploits become known to identify whether the exploit was used against the system. |  |
| 4. | CA-1 | Security Assessment and Authorization Policies and Procedures | * Ensures the system is properly assessed by an independent entity. |  |
| 5. | CM-1 | Configuration Management Policy and Procedures | * Ensures changes to the system’s security controls are only implemented following a change management capability. * Ensures all changes are authorized prior to implementation. * Ensures all changes are documented and tracked. |  |
| 6. | CP-1 | Contingency Planning Policy and Procedures | * Ensures contingency plans have been made for the system and are communicated to appropriate staff. |  |
| 7. | IA-1 | Identification and Authentication Policy and Procedures | * Ensures the identity of users with privileged access is appropriate before the account is issued. * Ensures the system enforces multi-factor authentication for privileged accounts. |  |
| 8. | IR-1 | Incident Response Policy and Procedures | * Ensures a capability exists for reporting security incidents. * Ensures a capability exists for responding to security incidents. |  |
| 9. | MA-1 | System Maintenance Policy and Procedures | * Ensures a capability exists for securely performing regular system maintenance. |  |
| 10. | MP-1 | Media Protection Policy and Procedures | * Ensures removable media is either explicitly prohibited or appropriately controlled when coming into contact with the system. |  |
| 11. | PE-1 | Physical and Environmental Protection Policy and Procedures | * Ensures only authorized individuals have physical access to the system. * Ensures the system is protected from environmental hazards such as fire, flood, earthquake, and disruption of utilities. |  |
| 12. | PL-1 | Security Planning Policy and Procedures | * Ensures security is appropriately designed and built into the system. |  |
| 13. | PS-1 | Personnel Security Policy and Procedures | * Ensures appropriate screening of CSP staff with logical or physical access to the system. * Ensures the citizenship of every staff member is known and is compliant with agency-specific citizenship requirements. |  |
| 14. | RA-1 | Risk Assessment Policy and Procedures | * Ensures the system is periodically checked for vulnerabilities. * Ensures known vulnerabilities are tracked via a Plan of Actions and Milestones (POA&M). * Ensures known vulnerabilities are resolved in a timely manner. |  |
| 15. | SA-1 | System and Services Acquisition Policy and Procedures | * Ensures development and acquisition activities are conducted in compliance with applicable Federal laws and regulations. |  |
| 16. | SC-1 | System and Communications Protection Policy and Procedures | * Ensures the system maintains appropriate separation of information. |  |
| 17. | SI-1 | System and Information Integrity Policy and Procedures | * Ensures information at rest and in transit is appropriately protected. * Ensures sensitive information, such as a user’s password, is protected with strong encryption mechanisms. |  |

## Attestation of Capabilities

The following capabilities exist and satisfy the associated requirement at least to the degree described in the associated attestation statement.

**Do not delete rows or modify the Attestation Statement column in the table below. State any exceptions in the Modifications column.**

Where the satisfaction of a control is partially or fully inherited, please check the appropriate box in the Modification Statement column. If there is no inheritance, leave both boxes unchecked. For example, if the PE controls are fully inherited from an underlying service provider with a separate authorization, check the “Inherited” box for each.

Please note, you are still attesting the statements for inherited controls are true to the best of your knowledge. If you have reason to believe otherwise, you must still state the difference in the Modification Statement column.

| **No** | **Control ID** | **Control Name** | **Attestation Statement** | **Modification Statement** |
| --- | --- | --- | --- | --- |
| 1. | AC-7 | Unsuccessful Login Attempts | * For privileged user accounts, the system locks the account for at least 15 minutes after three consecutive unsuccessful login attempts. | Inherited  Partially-Inherited |
| 2. | AC-20 | Use of External Information Systems | * Where information systems exist outside the authorization boundary and interconnect with this system, trust relationship terms and conditions exist and are in force with each external entity. | Inherited  Partially-Inherited |
| 3. | AT-2 | Security Awareness Training | * Security awareness training materials exist. * Secure awareness training materials are up-to-date and refreshed at least annually. * Every staff member undergoes security awareness training at least annually. | Inherited  Partially-Inherited |
| 4. | AT-3 | Role-Based Security Training | * Privileged users receive security training targeted to their role at least annually. | Inherited  Partially-Inherited |
| 5. | AT-4 | Security Training Records | * Security training records are maintained for at least one year. | Inherited  Partially-Inherited |
| 6. | AU-2 | Audit Events | * The system continuously logs for the following:   + Successful and unsuccessful account login attempts   + Account management events   + Object access, policy change   + Privilege functions, process tracking   + System events * For web applications, the system also continuously logs the following:   + All administrator activity   + Authentication checks   + Authorization checks   + Data deletions   + Data access   + Data changes   + permission changes * These event logs are reviewed on a regular basis as described in the Modification Statement column to the right. | Inherited  Partially-Inherited  Describe here the frequency with which event logs are reviewed. |
| 7. | AU-8 | Time Stamps | * The event logs generated above are time synchronized and time-stamped in coordinated universal time (UTC). | Inherited  Partially-Inherited |
| 8. | AU-9 | Protection of Audit Information | * The event logs are protected from unauthorized access, modification, and deletion. | Inherited  Partially-Inherited |
| 9. | AU-12 | Audit Generation | * All information system and network components generating logs as described in AU-2 above. | Inherited  Partially-Inherited |
| 10. | CA-2 (1) | Security Assessments, Independent Assessors | * An independent assessor has assessed the system with focus on the “Required” security controls. | Inherited  Partially-Inherited |
| 11. | CA-5 | Plan of Action and Milestones (POA&M) | * A POA&M for the system exists and is updated at least monthly in accordance with the *FedRAMP Tailored Continuous Monitoring Guide*. | Inherited  Partially-Inherited |
| 12. | CM-2 | Baseline Configuration | * The configuration of the system is fully documented and maintained. * It is up-to-date at this time. | Inherited  Partially-Inherited |
| 13. | CM-7 | Least Functionality | * The system is configured to only allow documented and authorized functionality. * A list of prohibited or restricted functions, ports, protocols, and/or services exists. * The list is consistently enforced across the system, especially at the perimeter. | Inherited  Partially-Inherited |
| 14. | IA-2 | Identification and Authentication (Organizational Users) | * Privileged users are consistently authenticated by two or more authentication factors (something the user is, something the user has, something the users knows). | Inherited  Partially-Inherited |
| 15. | IA-4 | Identifier Management | * Unique identifiers are assigned to each user, device, and service account. * Identifiers are not re-used for at least two years. * Identifiers are disabled after 90 days of inactivity. | Inherited  Partially-Inherited |
| 16. | IA-5 | Authenticator Management | * Authenticators are refreshed every 60 days. | Inherited  Partially-Inherited |
| 17. | IA-5 (1) | Authenticator Management | Password-Based Authentication | * Passwords are case sensitive. * A mechanism ensures passwords are a minimum of twelve characters, with at least one each of upper-case letters, lower-case letters, numbers, and special characters. * At least one character in the password must change for a new password to be accepted. * The user is prevented from re-using their previous 24 passwords. * A user must wait at least one day between password changes. A user must change their password within 60 days. | Inherited  Partially-Inherited |
| 18. | IA-7 | Cryptographic Module Authentication | * The authentication cryptographic module is FIPS 140-2 validated with an issued certificate number. | Inherited  Partially-Inherited |
| 19. | IA-8 | Identification and Authentication (Non-Organizational Users) | * Non-organizational users, systems, and services are each uniquely identified within the system. | Inherited  Partially-Inherited |
| 20. | IA-8 (3) | Identification and Authentication (Non-Organizational Users) | Acceptance of FICAM-Approved Products | * The system is able to integrate with other Federal Identity, Credential, and Access Management (FICAM)-approved identity management capabilities. | Inherited  Partially-Inherited |
| 21. | IA-8 (4) | Identification and Authentication (Non-Organizational Users) | Use of FICAM-Issued Profiles | * The information system conforms to FICAM-issued profiles. | Inherited  Partially-Inherited |
| 22. | IR-2 | Incident Response Training | * Administrators receive incident response training at least annually. | Inherited  Partially-Inherited |
| 23. | IR-5 | Incident Monitoring | * For each security incident identified, incident response staff track it to closure. | Inherited  Partially-Inherited |
| 24. | IR-7 | Incident Response Assistance | * Incident response resources and capabilities are available to users of the system who may have experienced a security incident. | Inherited  Partially-Inherited |
| 25. | IR-8 | Incident Response Plan | * An Incident Response Plan exists. * The Incident Response Plan is reviewed at least annually and updated as needed. * The incident response plan ensures the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US CERT) is notified of security incidents consistent with their reporting requirements. | Inherited  Partially-Inherited |
| 26. | IR-9 | Information Spillage Response | * A capability exists for prompt and secure removal of sensitive or classified information from the system in the event of an information spill. | Inherited  Partially-Inherited |
| 27. | MA-2 | Controlled Maintenance | * System maintenance is regularly scheduled and performed. * All maintenance activities require an approval, and are monitored. * Maintenance records are consistently maintained. * Whenever a maintenance activity impacts a security control, the control is always tested at the conclusion of the maintenance to ensure it is still functioning properly. | Inherited  Partially-Inherited |
| 28. | MA-4 | Non-local Maintenance | * Non-local maintenance activities require an approval and are monitored. * Non-local maintenance sessions are terminated upon completion of the maintenance activity. | Inherited  Partially-Inherited |
| 29. | MA-5 | Maintenance Personnel | * A process exists for authorizing maintenance personnel. * A list of authorized maintenance personnel exists and is maintained. * Unauthorized personnel performing maintenance are supervised by authorized personnel. | Inherited  Partially-Inherited |
| 30. | MP-2 | Media Access | * Removable media is strictly prohibited within the system’s authorization boundary. | Inherited  Partially-Inherited |
| 31. | MP-6 | Media Sanitization | * Any component used within the authorization boundary is securely sanitized upon removal from the system, prior to disposal or re-use. | Inherited  Partially-Inherited |
| 32. | MP-7 | Media Use | * Users are prohibited from attaching media to the system. | Inherited  Partially-Inherited |
| 33. | PE-2 | Physical Access Authorizations | * A process exists for authorizing physical access to the system for personnel. * A list of authorized personnel with physical access exists and is maintained. * The list is reviewed and adjusted at least annually. * Authorized personnel are issued credentials for facility access. * Unauthorized personnel requiring physical access are supervised by authorized personnel. | Inherited  Partially-Inherited |
| 34. | PE-3 | Physical Access Control | * Physical access controls are in place and enforcing physical access rights. * Access audit logs are maintained for all individuals entering and exiting the facility. * A physical inventory of assets is maintained. * The physical asset inventory is reviewed at least annually for accuracy. | Inherited  Partially-Inherited |
| 35. | PE-6 | Monitoring Physical Access | * Physical access is monitored. * Physical access logs are reviewed at least monthly. | Inherited  Partially-Inherited |
| 36. | PE-8 | Visitor Access Records | * Visitor logs for physical access are maintained for at least one year, and reviewed at least monthly. | Inherited  Partially-Inherited |
| 37. | PE-12 | Emergency Lighting | * Emergency lighting is deployed in each facility, which activates automatically in the event of a power outage or disruption. * Emergency lighting covers emergency exits and evacuation routes within each facility. | Inherited  Partially-Inherited |
| 38. | PE-13 | Fire Protection | * A fire detection and suppression capability exists to protect the system. * The fire detection and suppression capability is supported by an independent energy source. | Inherited  Partially-Inherited |
| 39. | PE-14 | Temperature and Humidity Controls | * The temperature and humidity of the system’s physical environment is monitored continuously. * The temperature and humidity of the system’s physical environment is maintained consistent with the American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments. | Inherited  Partially-Inherited |
| 40. | PE-15 | Water Damage Protection | * To protect the system from water damage, the facilities where the system is housed have master shutoff or isolation valves that are accessible, working properly, and known to key personnel. | Inherited  Partially-Inherited |
| 41. | PE-16 | Delivery and Removal | * Authorize, monitor, and control all information system components entering and exiting the facilities where the system is housed, and keep records of those items. | Inherited  Partially-Inherited |
| 42. | PL-4 | Rules of Behavior | * The rules of behavior for staff in contact with the system exists and is updated at least every three years. * Every staff member reads and signs the rules of behavior before receiving access to the system. | Inherited  Partially-Inherited |
| 43. | PS-4 | Personnel Termination | * All access to the system is disabled and revoked the same day a staff member is terminated. * All information and resources formerly controlled by the terminated individual is retained by another authorized staff member. | Inherited  Partially-Inherited |
| 44. | PS-5 | Personnel Transfer | * All access to the system is disabled and revoked within 24 hours following the formal transfer action for DoD customers or within five days for non-DoD customers. * All information and resources formerly controlled by the transferred individual is retained by another authorized staff member. | Inherited  Partially-Inherited |
| 45. | PS-6 | Access Agreements | * Access agreements exist for every role a staff member may hold relative to the system. * The access agreements are reviewed and updated at least annually. * Every staff member with access to the system signs an access agreement appropriate for the staff member’s role or level of access. | Inherited  Partially-Inherited |
| 46. | PS-7 | Third-Party Personnel Security | * All third-party security personnel are treated as CSP employees. | Inherited  Partially-Inherited |
| 47. | PS-8 | Personnel Sanctions | * Formal sanctions exist and are employed for individuals failing to comply with established information security policies and procedures. | Inherited  Partially-Inherited |
| 48. | SA-2 | Allocation of Resources | * An adequate budget exists to address security requirements for this system. * Adequate staff are dedicated to the security of this system. | Inherited  Partially-Inherited |
| 49. | SA-3 | System Development Life Cycle (SDLC) | * The system is maintained using an existing SDLC methodology and capability, which incorporates security considerations throughout the lifecycle. | Inherited  Partially-Inherited |
| 50. | SA-4 | Acquisition Process | * An acquisition process exists and ensures components and services acquired for the system meet all relevant security requirements and regulations. | Inherited  Partially-Inherited |
| 51. | SA-4 (10) | Acquisition Process | Use of Approved Personal Identity Verification (PIV) Products | * All components acquired in support of PIV requirements are on the FIPS 201-approved products list. | Inherited  Partially-Inherited |
| 52. | SA-5 | Information System Documentation | * Administrator documentation exists for the information system, all system components, and all system services. * The documentation describes the secure configuration, installation, and operation. | Inherited  Partially-Inherited |
| 53. | SC-20 | Secure Name /Address Resolution Service (Authoritative Source) | * The system or supporting infrastructure provides additional validation of the authoritative name resolution data returned by the system in response to external name/ address resolution, such as Domain Name System Security Extensions (DNSSEC). | Inherited  Partially-Inherited |
| 54. | SC-21 | Secure Name /Address Resolution Service (Recursive or Caching Resolver) | * The system or supporting infrastructure performs additional validation of name/address resolution responses received from authoritative sources, such as DNSSEC. | Inherited  Partially-Inherited |
| 55. | SC-22 | Architecture and Provisioning for Name/ Address Resolution Service | * Collectively, the name/address resolution service is fault-tolerant and appropriately works within the fault-tolerant aspects of the system. | Inherited  Partially-Inherited |
| 56. | SC-39 | Process Isolation | * The system maintains a separate execution domain for each executing process and customer instance. | Inherited  Partially-Inherited |
| 57. | SI-5 | Security Alerts, Advisories, and Directives | * System administrators or incident response staff receive security alerts from all vendors represented within the system, as well as from DHS US CERT. * Our incident response staff create and disseminate security alerts and advisories to system administrators, appropriate staff, and users of the system. | Inherited  Partially-Inherited |
| 58. | SI-12 | Information Handling and Retention | * Information in the system is retrained in compliance with the National Archives & Records Administration (NARA) Records Schedule. * Information within the system is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | Inherited  Partially-Inherited |
|  |  |  |  |  |
| 59. | Citizenship | n/a | * Staff members with access to the system include:   *Check boxes to the right.* | Check all that apply:  US Persons  Non-US Persons |
| 60. | Geography | n/a | * All components of the system reside:   *Check boxes to the right* | Check one:  Fully within the United States  Partially or fully outside the United States |