Universal Service Administrative Co.

ATTACHMENT 3 – SECURITY AND CONFIDENTIALITY PROCEDURES

Security Requirements for IT Acquisition Efforts

This document provides security and privacy requirements for an external information system (USAC owned and contractor operated or contractor owned and operated on behalf of USAC), and Cloud Information Systems. Cloud Information Systems includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS). It also requires the system to be FedRAMP authorized prior to production go live. The security and privacy requirements are appropriately formatted to allow the respective security and privacy contract language to be placed in-line within a statement of work for each system type. The security and privacy requirements identified in this document will ensure compliance with the appropriate provisions of Federal Information Security Modernization Act of 2014 (FISMA of 2014), OMB Circular A-130, and NIST Special Publication (SP) 800-53, Revision 5 or latest version.

IT Security Requirements

Information systems supporting USAC must meet the minimum security and privacy requirements through the use of security controls in accordance with NIST Special Publication 800-53, Revision 5 or latest version (hereafter described as NIST 800-53), "Security and Privacy Controls for Federal Information Systems and Organizations".

- The contractor shall comply with all applicable Federal Laws and Regulations.
- The contractor shall comply with all applicable Federal Information Processing Standards (FIPS). NIST Special Publications (SP) (800 Series) and guidance.
- The contractor shall comply with all applicable USAC Policies.
- The contractor shall apply the appropriate set of Low, Moderate, or High impact baseline security controls in NIST 800-53, as determined by USAC based in accordance with FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems".
- NIST 800-53 controls requiring organization-defined parameters (i.e., password change frequency) shall be consistent with USAC specifications.
- The Contractor shall use USAC technical guidelines, NIST guidelines, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening their systems.

Assessment and Authorization (A&A) Activities

The Contractor system/application must have a valid assessment and authorization, known as an Authority to Operate (ATO) before going into operation and processing USAC information. The failure to obtain and maintain a valid ATO may result in the termination of the contract. The system must have a new A&A Activities conducted when there is a significant change to the system's security posture or via continuous monitoring based on USAC Information Security Continuous Monitoring Strategy, which is reviewed and accepted by the USAC CISO.

Assessing the System

1. The Contractor shall comply with the A&A requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall fully support USAC IT security in the development and execution of the following A&A documentation and activities:
   - System Security Plan (SSP) per NIST SP 800-54 Revision 5
   - Contingency Plan, Training and Testing
   - Configuration Management Plan.
   - Penetration Testing
2. At the Moderate impact level and higher, USAC will conduct an independent Security Assessment in accordance with NIST SP 800-37.
   - The Contractor shall support assessment activities to include:
   - Preparation and review of documentation
   - Participation in interviews and meetings during the assessment
   - Scheduling to support assessment of the functionally complete system
   - Remediation of draft findings during the assessment
3. Identified gaps between required NIST 800-53 controls and the contractor's implementation as documented in the Security Assessment Report (SAR) as result of the security assessment or as result of Penetration Testing shall be tracked for mitigation in USAC's Plan of Action and Milestones (POA&M) system in accordance with USAC procedures. All gaps identified with a severity of Critical or High shall be remediated before an Authorization to Operate is accepted, and lower severity gaps shall be required unless accepted as POA&Ms by the USAC CISO.

4. The system shall be subject to USAC vulnerability and configuration scanning for all components deployed on USAC premise or on USAC cloud infrastructure that is provided by a FedRAMP Cloud Service Provider as IaaS.

5. The system shall support USAC's SEIM, Splunk, for continuous logging and monitoring.

6. The system shall support Okta and the System for Cross-domain Identity Management (SCIM) for integration.

7. The ATO decision is made by the USAC Authorizing Official (AO) on advice of the USAC Chief Information Security Officer (CISO) based on analysis of the security and privacy risks of the system, the findings of the security assessment, and findings of the penetration tests. No system shall be deployed to production for live management of USAC data without authorization by the AO.

Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The contractor shall also protect all USAC data, equipment, etc. by treating the information in accordance with its FISMA system categorization.

All information about the systems gathered or created under this contract should be considered as SBU information. If contractor personnel must remove any information from the primary work area that is included in the ATO boundary, they should protect it to the same security requirements. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

When no longer required, this information, data, and/or equipment shall be returned to USAC control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, "Guidelines for Media Sanitization".

USAC will retain unrestricted rights to USAC data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

The data must be available to USAC upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to USAC.