Universal Service Administrative Co.

ATTACHMENT 9 – 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 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.

External Information Systems – 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 create, maintain and update the following A&A documentation:
   - System Security Plan (SSP) completed in accordance with NIST SP 800-18, Revision 1 or the most recent version.
   - Contingency Plan (including Disaster Recovery Plan) completed in accordance with NIST SP 800-34, the most recent version.
   - Contingency Plan Test Report.
   - Incident Response Plan completed in accordance with NIST SP 800-61, "Computer Security Incident Handling Guide" the most recent version.
   - Incident Response Test Report completed in accordance with NIST SP 800-61, "Computer Security Incident Handling Guide" the most recent version.
   - Configuration Management Plan.
   - Plan of Actions & Milestones.
   - Penetration Test Reports documenting the results of vulnerability analysis and exploitability of identified vulnerabilities.
2. At the Moderate impact level and higher, the **Contractor** is responsible for providing an independent Security Assessment/Risk Assessment in accordance with and NIST SP 800-37.
3. Identified gaps between required NIST 800-53 controls and the contractor's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a POA&M document completed in accordance with USAC Security Procedural POA&M Guide. Depending on the severity of the gaps, USAC may require them to be remediated before an Authorization to Operate is accepted.

Authorization of the System

1. Upon receipt of the documentation (Security Authorization Package (SAP)) USAC Authorizing Official in collaboration the CISO, will render an acceptance decision to:
   - Allow system operation w/out any restrictions or limitations on its operation;
   - Allow system operation w/restriction or limitation on its operation, or;
   - Not allow for operation.
2. The Contractor shall provide access to USAC, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Security Program. At its option, USAC may choose to conduct on site surveys. The Contractor shall make appropriate personnel available for interviews and documentation during this review. If documentation is considered proprietary or sensitive, these documents may be reviewed on-site under the hosting Contractor's supervision.

Reporting and Continuous Monitoring

Through continuous monitoring, security controls and supporting deliverables are updated and submitted to USAC per the agreed upon schedule. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow USA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

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.