Interconnection Security Agreement

Between

Universal Service Administrative Company ("USAC")

&

SERVICE PROVIDER

Governing Interconnection Between

USAC National Lifeline Accountability Database and/or National Verifier ("NLAD and/or NV")

&

Service Provider System ("Acronym")

Date: February 23, 2023

INTERCONNECTION SECURITY AGREEMENT

Document Information

USAC Primary Point of Contact	
Name	Joseph Ho, Senior Manager of Product Management
Contact Number	202-572-5661
E-mail Address	Joseph.Ho@usac.org
SERVICE PROVIDER Point of Contact	
Name	
Contact Number	
E-mail Address	

Version History

Version	Date	Description
1.0	XX/XX/2020	First Version signed by USAC and Service Provider
2.0	11/23/2020	Template modified with updated language
3.0	2/23/2022	Template modified to reflect the transition of EBBP to ACP

Distribution List			
Name	**Title**	**Agency/Office**	**Contact Information**
SERVICE PROVIDER OFFICIAL			
SERVICE PROVIDER OFFICIAL			
Timothy O'Brien	Vice President of Lifeline	USAC	Tim.OBrien@usac.org
Jeremy Hayes	Chief Information Security Officer	USAC	Jeremy.Hayes@usac.org

Interconnection Security Agreement Authorization

We have carefully reviewed the Interconnection Security Agreement ("ISA") between UNIVERSAL SERVICE ADMINISTRATIVE COMPANY ("USAC"), a not-for-profit corporation organized under the laws of Delaware, and SERVICE PROVIDER ("Acronym") (collectively, Parties). This document has been completed in accordance with the requirements set forth in National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-47, *Security Guide for Interconnecting Information Technology Systems*. This agreement will be reviewed annually and will be re-signed by all Parties on a yearly basis. This ISA, dated MONTH [•], YEAR (the "Effective Date"), is between USAC and SERVICE PROVIDER.

USAC

_____ _____

Jeremy Hayes DATE

Chief Information Security Officer

SERVICE PROVIDER OFFICIALS

_____ _____

Official's name

Title DATE

_____ _____

Official's name (optional) DATE

Title (optional)

Table of contents

1. INTRODUCTION

A system interconnection is defined as the direct connection of two or more information technology ("IT") systems for the purpose of sharing data and other information resources. An interconnection security agreement (ISA") is used to document connections between systems to exchange information. The ISA is much more than a contract or service agreement between two organizations; the ISA is a security agreement that protects both interconnected systems from each other. The intent behind an ISA is to detail some basic system information and then to document and agree on how the security of the two systems will be maintained. Significant benefits that can be realized through a system connection include: reduced operating costs, greater functionality, improved efficiency, and centralized access to data. Interconnecting IT systems may also strengthen ties among participating organizations by promoting communication and cooperation.

The requirements for interconnection between USAC and [SERVICE PROVIDER] are for the express purpose of connecting and exchanging data between:
(A) USAC's pre-production and production environment servers for the National Lifeline Accountability Database ("NLAD") and the National Verifier ("NV") Systems owned by USAC and controlled by USAC, and
(B) the SERVICE PROVIDER's development and production environment servers controlled by SERVICE PROVIDER.

SERVICE PROVIDER will access an application programming interface ("API") connection to NLAD and/or NV Systems to confirm an applicant's eligibility for the federal Lifeline program and/or the Affordable Connectivity Program ("ACP") benefits in order to query against the database of enrolled subscribers to ensure the applicant does not already receive the benefit(s). The expected benefits of the connection are to reduce waste, fraud, and abuse; ensure applicants are eligible to receive the federal Lifeline program and/or ACP benefits; and prevent subscribers from receiving duplicate benefits.

2. Connection Purpose

2.1 System Identification

System A:
USAC, National Verifier ("NV")
Federal Information Processing Standards ("FIPS") 199 Categorization: **Moderate**
Authority to Operate ("ATO") Date:
System Owner Name: Timothy O'Brien
Contact Number: 202-772-4520
Email Address: Tim.OBrien@usac.org

System B:
USAC, National Lifeline Accountability Database ("NLAD")
FIPS 199 Categorization: **Moderate**
Authority to Operate ("ATO") Date:
System Owner Name: Timothy O'Brien
Contact Number: 202-772-4520
Email Address: Tim.OBrien@usac.org

System C:
Service Provider, System
FIPS 199 Categorization: **Moderate**
System Owner Name:
Contact Number:
Email Address:

2.2 Connection Purpose and Information Shared/Passed:
This connection between the NV and/or NLAD pre-production and production environment servers and the SERVICE PROVIDER servers, owned by SERVICE PROVIDER, is a two-way path. The interconnection between USAC and SERVICE PROVIDER is for the express purpose of exchanging data between the two systems to verify that the applicant is currently eligible for the Lifeline and/or ACP benefits and/or does not receive duplicate benefits.

2.3 Information Sensitivity

Services Offered. Connectivity will be used for SERVICE PROVIDER to transmit personally identifiable information ("PII") of applicants to USAC, to enable USAC to confirm, with an affirmative or negative confirmation, whether the applicant is already enrolled in the federal Lifeline program benefit and/or ACP benefits, and/or is eligible to receive the Lifeline and/or ACP benefits. Affirmative consent must be obtained from the applicant by SERVICE PROVIDER prior to the submission of PII to USAC as described in the relevant Federal Communications Commission ("FCC") application (i.e., Form 5629, Lifeline Program Application Form or Form 5645 Affordable Connectivity Program Application Form), so that USAC can confirm the applicant's eligibility through available data sources. PII that is authorized to be transmitted via the interconnection is limited to the following:

i) Applicant's name (first and last);
ii) Last 4 digits of Applicant's Social Security Number ("SSN");
iii) Applicant's Tribal ID (if applicable);
iv) Applicant's date of birth;
v) Applicant's primary and/or mailing address; and
vi) Application ID.

If additional PII is needed to verify an applicant's eligibility, this Agreement also authorizes the following data to be transmitted:

i) Applicant's phone number;
ii) Applicant's email address;
iii) Benefit qualifying person's name (first and last);
iv) Last 4 digits of Benefit qualifying person's SSN;
v) Benefit qualifying person's Tribal ID; and
vi) Benefit qualifying person's date of birth.

Data Sensitivity. The sensitivity of data exchanged between USAC and SERVICE PROVIDER is not to exceed a moderate security categorization. This data must be protected using FIPS Publication 140-2 (or FIPS Publication 140-3 if applicable) certified encryption standards..

3. Connection Specifics

3.1 Connection Method

The security of the information being retrieved by SERVICE PROVIDER from USAC shall be protected in accordance with the Federal Information Security Modernization Act of 2014, as amended ("FISMA") and NIST requirements. The connections at each end must be located within controlled access facilities, guarded twenty-four (24) hours a day. Interconnections utilizing Internet VPN technologies may be terminated on shared infrastructure equipment that is not isolated from the Internet. VPN transmission protocol/internet protocol ("TCP/IP") traffic to USAC is internet protocol security ("IPSEC") encrypted using advanced encryption standards ("AES") 128 encryption or stronger. There may be for a specific system critical seasonality or performance considerations (e.g., a filing window or specific time of the year or day when system performance is expected to be constrained) during when USAC requests the SERVICE PROVIDER to avoid access.

4. System Vulnerabilities

One system's vulnerabilities can have an adverse impact on the security of another system, especially when the two systems are connected and sharing information. Because of this, the system owners and the security officers must be aware of the identified vulnerabilities of all the systems that are connected to their system. Special attention should be paid to any moderate or high vulnerabilities. With this in mind, the system owners of both systems agree that any new vulnerabilities categorized as moderate or higher risk will immediately be communicated to the other system's owner/security officer.

5. Incident Reporting

USAC and SERVICE PROVIDER agree to report and track incidents in accordance with the PII breach reporting requirements as set forth in Office of Management and Budget ("OMB")

Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (2017).

- SERVICE PROVIDER will promptly notify these contacts at USAC simultaneously:
  - USAC Privacy, privacy@usac.org.
  - USAC IT Security Operations, incident@usac.org.
- USAC will promptly notify this contact at SERVICE PROVIDER:
  - SERVICE PROVIDER [TO FILL OUT]
- As soon as possible after notifying SERVICE PROVIDER of an incident, or receiving notification of an incident from SERVICE PROVIDER, USAC will notify the FCC's Network Security Operations Center ("NSOC") at NSOC-Monitor@fcc.gov or (202) 418-4011 of incidents within one (1) hour of notification.

If the Party experiencing the incident cannot contact the other Party's System Security Contacts within one (1) hour, or if contacting the System Security Contact is not practical, then this contact information shall be used:

- USAC Manager of Security Operations - (202) 772-4511
- SERVICE PROVIDER [TO FILL OUT]

USAC and SERVICE PROVIDER agree to notify all the Security Contact(s) named in this Agreement as soon as possible, but no later than one (1) hour, after the discovery of a breach (or suspected breach) involving PII. The Party that experienced the incident will also be responsible for following its internal established procedures, including:

- Notifying the proper organizations (e.g., Information Systems Security Officers (ISSOs"), and other contacts listed in this document);

- Conducting a breach and risk analysis, and making a determination of the need for notice and/or remediation to individuals affected by the loss; and

- Providing such notice and credit monitoring at no cost to the other Party, if the analysis conducted by the Party having experienced the loss incident indicates that individual notice and credit monitoring are appropriate.

In the event of any incident arising from or in connection with this Agreement, each Party will be responsible only for costs and/or litigation arising from a breach of the Party's own systems; USAC is responsible only for costs and litigation associated with breaches to USAC systems and

SERVICE PROVIDER is responsible only for breaches associated with SERVICE PROVIDER systems.

USAC shall not be liable to SERVICE PROVIDER or to any third person for any cause of action arising from the possession, control, or use by SERVICE PROVIDER of applicant or subscriber PII, or for any loss, claim, damage or liability, of whatever kind or nature, which may arise from or in connection with this Agreement or using applicant or subscriber PII.

SERVICE PROVIDER shall not be liable to USAC or to any third person for any cause of action arising from the possession, control, or use by USAC of applicant or subscriber PII, or for any loss, claim, damage or liability, of whatever kind or nature, which may arise from or in connection with this Agreement or using applicant or subscriber PII.

6. Backups/Updates/Changes

USAC performs backups of its various systems with in-house database administrators ("DBAs") in accordance with USAC procedures. Planned technical changes to system architecture that directly impact one or more of the applications or system resources used to interface with the other Party will be reported by email to the Technical Point of Contact (see Section 11) no later than thirty (30) days before such changes are implemented. If applicable, the initiating Party agrees to conduct a risk assessment based on the new system architecture. If applicable, the Parties will amend the terms of this ISA to reflect such changes not later than thirty (30) days after implementation. If USAC is updating the table structures, the SERVICE PROVIDER System Owner and Technical Points of Contact must be notified one month (30 days) prior to the change. Any change to the transfer method or source of data shall be communicated to both System Owners and to the Technical Points of Contact via email.

7. User Community

Access will be granted to only USAC and SERVICE PROVIDER users who require access to the NV and/or NLAD to perform their responsibilities and duties and who have been informed of and agree in advance and in writing that they will abide by the terms of this agreement. Access by USAC and SERVICE PROVIDER users must be based upon a need-to-know for a legitimate and authorized business purpose. Privileges granted by USAC and SERVICE PROVIDER must also comply with the principles of separation of duties and of least privilege. *See* OMB Circular A-130; National Institute of Standards and Technology ("NIST") Special Publication 800-53, (current version), controls AC-5 and AC-6, including the Supplemental Guidance (including any amendments published by OMB or NIST after the effective date of this Agreement). No access will be granted to one or more of the interconnections or their associated applications or system resources unless authorized by the owner of the resource or application in accordance with the terms in this ISA. USAC and SERVICE PROVIDER users' access must be limited to the least amount of access required to perform the assigned authorized tasks.

7.1 Information Exchange Security

All data transferred between systems will be encrypted over secure web interfaces via the authorized API connection maintained by USAC. The user agent requesting access must be capable of accepting cookies and following all HTTP redirects. Only authenticated requests through an encrypted channel which will be submitted using the HTTPS ("SSL/TLS"), will be accepted. The connection authorization mechanism restricts each authenticated API user to only the data related to the companies (i.e. study area codes in NLAD) assigned to them as well as restricting them to specific API operations and resources that are provisioned by USAC. The security of the information being passed on these two-way connections will be protected in accordance with requirements set forth in this ISA. Both parties agree to maintain the connections at each end in a controlled access environment that includes the use of authorized access codes (passwords or public key infrastructure ("PKI")) to restrict access and to safeguard the data by utilizing encryption for data in transit and at rest.

8. Rules of Behavior

USAC's system and users are expected to protect SERVICE PROVIDER's system. SERVICE PROVIDER's system and employees (including contractors and subcontractors) with access to the system interconnection are expected to protect USAC's pre-production and production environment servers for the NV and/or NLAD in accordance with the FISMA, the Privacy Act (5 U.S.C. § 552a), the Trade Secrets Act (18 U.S.C. § 1905), the Unauthorized Access Act (18 U.S.C. § 2701), and NIST and OMB requirements. In addition, SERVICE PROVIDER may not take actions that impose an unreasonable or disproportionately large load on the infrastructure of the NV and/or NLAD system connections and USAC reserves the right to limit or stop connection transaction rates in order to safeguard USAC's systems during peak system transaction volumes or for system maintenance activities.

9. Controls

This ISA must comply with all security policies and standards applicable to the SERVICE PROVIDER and USAC's Terms and Conditions (including updates to those requirements). However, changes may occur as the security landscape changes and evolves. Both Parties also will inform the other by email of planned changes to the security landscape no later than thirty (30) days before such changes are implemented. If applicable, the initiating Party agrees to conduct a risk assessment based on the new security landscape. If applicable, the Parties will amend the terms of this ISA to reflect such changes not later than thirty (30) days after implementation. Specific Controls that may need to be maintained between USAC and SERVICE PROVIDER include, but are not limited to the following:

AC-2 Account Management, AC-17 Remote Access; AU-6 Audit Review, Analysis and Reporting; SC-8 Transmission Confidentiality and Integrity; SC-7 Boundary Protection;

IA-2 Identification and Authentication; IR-8 Incident Response Plan; RA- 3 Risk Assessment, CM-3 Configuration Change Control.

Both parties shall maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained on the system with the highest sensitivity levels. Neither party shall release, publish, or disclose information to unauthorized personnel, and shall protect such information using best practices that align with the FISMA, Privacy Act (5 U.S.C. § 552a), Trade Secrets Act (18 U.S.C. § 1905), Unauthorized Access Act (18 U.S.C. § 2701), and NIST and OMB requirements

10. Cost Considerations

There will be no cost sharing or payments exchanged between USAC and the SERVICE PROVIDER for any of these interconnections.

11. Material Changes to System Configuration

Planned technical changes to system architecture that directly impact one or more of the applications or system resources used to interface with the other Party will be reported to Technical Point of Contact (below) no later than thirty (30) days before such changes are implemented. If this ISA is affected by the change to the system architecture, the initiating Party agrees to conduct a risk assessment based on the new system architecture and its impact on this ISA before the change is implemented. If the terms of this ISA need to be changed as a result of the impact assessment, the Parties will amend the terms prior to the implementation of the material system change.

11.1 New Connection.
The initiating Party will notify the other Party at least thirty (30) days before it connects its system with any other system, including systems that are owned and operated by third parties, that directly impacts one or more of the applications or system resources used to interface with the other Party or has the potential to send traffic across one or more of the connections covered in this ISA. If this ISA is affected by the change to the system architecture, the initiating Party agrees to conduct a risk assessment based on the new system architecture and its impact on this ISA before the change is implemented. If the terms of this ISA need to be changed as a result of the impact assessment, the Parties will amend the terms prior to the implementation of the material system change.

A Party's Technical Point of Contact should be immediately notified if there is a change that requires an immediate response. The method of communication between the two parties will be via email.

USAC Technical Point of Contact	
Name	Joseph Ho, Senior Manager of Product Management
Contact Number	202-572-5661
E-mail Address	Joseph.Ho@usac.org
Service Provider Technical Point of Contact	
Name	
Contact Number	
E-mail Address	

12. Personnel Changes

The Parties agree to inform the other by email of the separation or long-term absence (30 days or more) of their respective System Owner or Technical Point of Contact. In addition, both Parties will inform the other by email of any changes in System Owner or Technical Point of Contact information. Both Parties also will inform the other by email of changes to user profiles, including applicable users who resign or change job responsibilities that have access to the interconnection.

13. Audit Trail Responsibilities

Both Parties are responsible for auditing and monitoring their own application processes and user activities involving these interconnection activities that will be recorded, including event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs will be retained for a minimum of three (3) years.

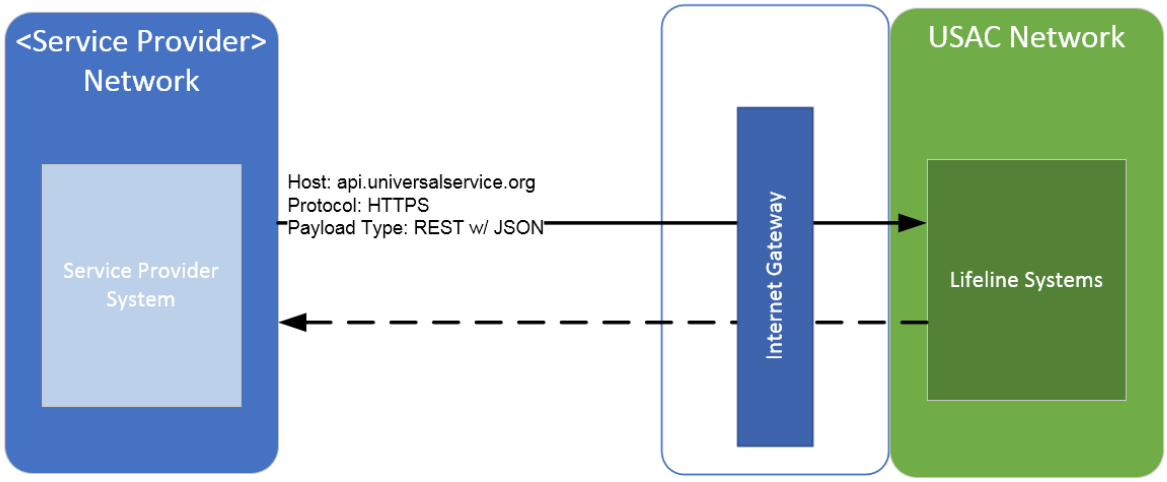
14. Representations

USAC is designated by the FCC as the permanent Administrator of the federal Universal Service Fund ("USF") support mechanisms, 47 C.F.R. §§ 54.701-54.717. Under the FCC's rules and the Memorandum of Understanding between the FCC and USAC ("FCC/USAC MOU"), USAC administers each of the USF programs consistent 47 U.S.C. § 254 and 47 C.F.R. Part 54, other laws as applicable, and orders, written directives, and other instructions promulgated by the FCC or its bureaus and offices. USAC collects and verifies eligibility of Lifeline program subscriber data under 47 U.S.C. § 254 and 47 C.F.R. Part 54 Subpart E. As part of its administration of the Lifeline program, USAC developed, and is the owner of, the NLAD and NV Systems. Under an additional Memorandum of Understanding between the FCC and USAC (Nov. 16, 2021)

("FCC/USAC ACP MOU")[1], USAC is authorized to oversee the administration of the ACP, and to leverage the existing NLAD and NV systems to administer the ACP. USAC is authorized to enter into this ISA with SERVICE PROVIDER.

SERVICE PROVIDER warrants that it is authorized to enter into this ISA with USAC.

15. Topological Drawing



16. Timeline

This agreement is valid for one (1) year after the last date on either signature above. It will subsequently be updated, reviewed, and reauthorized by that date annually. USAC will notify SERVICE PROVIDER prior to the expiration of this Agreement. Failure to re-sign the ISA could result in termination of API access to NLAD and/or NV systems. Either party may terminate this ISA upon thirty (30) days' advance notice to the System Owners in writing or at any time in the event of a security incident that necessitates an immediate response. In the event a party breaches this Agreement, that party shall be given 30 days to cure from date of notice of the breach.

[1] Memorandum of Understanding between the Federal Communications Commission and the Universal Service Administrative Company Regarding the Affordable Connectivity Program, available at https://www.fcc.gov/sites/default/files/affordable-connectivity-program-mou-fcc-usac-11162021.pdf.