SECURITY ADDENDUM for SERVICE PROVIDERS

This Consolidated Security Addendum for Vendors and Third-Party Representatives ("**Security Addendum**") is incorporated by refence into and forms part of the Master Purchase Agreement ("MPA"), Master Services Agreement ("MSA"), Master Representative Agreement ("MRA"), Statement of Work ("SOW"), or Service, Product, or Purchase Order ("Order") (together with any appendices, exhibits, annexes, or amendments thereto, the "**Agreement**") executed between Consolidated Communications, Inc. ("**Consolidated**") and the vendor, service provider, contractor, third-party representative, or supplier ("**Service Provider** ") indicated in the applicable Agreement. Consolidated enters into this Security Addendum on its own behalf and on behalf of its Affiliates.

1. Definitions. Capitalized terms used in this Security Addendum shall have the meanings set forth in this Security Addendum. Capitalized terms used but not otherwise defined herein shall have the meanings given to them in the Agreement.

1.1 "**Access**" means (a) to enter a location; or (b) to obtain, read, copy, edit, divert, release, affect, alter the state of, or otherwise view data or systems in any form, including through information technology (IT) systems, cloud computing platforms, networks, security systems, and equipment (software and hardware).

1.2 "**Affiliate**" means all entities that Control, are Controlled by, or are under common Control with a Party, where "**Control**" means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of an entity, whether through the ownership of at least fifty percent (50%) of its voting securities, by contract, or otherwise. Consolidated "Affiliates" are limited to subsidiaries under the direct and indirect Control of Consolidated Communications.

1.3 "**Consolidated Data**" means all data and information in any form or media provided to, received by, accessed by, or made available to Service Provider or Service Provider Personnel directly or indirectly from or on behalf Consolidated, or otherwise in connection with the Agreement, including (a) any transformations, improvements, combinations and derivative works thereof and (b) CPNI, U.S. Records, and data about or related to Consolidated, Consolidated customers, or the use of Consolidated products and services. All Consolidated Data is the Confidential Information of Consolidated.

1.4 "**Customer Proprietary Network Information**" or "**CPNI**" means (a) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of Consolidated; and information contained in the bills pertaining to their voice services or (b) as otherwise defined by 47 U.S.C. §222(h)(1).

1.5 "**Data Privacy Laws**" means all United States federal, state, or local laws and regulations relating to Personal Data, as they may be amended or replaced. Data Privacy Laws includes laws and regulations that are enacted or become effective after the Effective Date.

1.6 "**Data Subject**" means the identified or identifiable natural person to whom the Personal Data relates and includes any similarly defined term under Data Privacy Laws.

1.7 "**Domestic Communications**" or "**DC**" means: (a) Wire Communications or Electronic Communications, as defined by 18 U.S.C. § 2510, (whether stored or not), from one location within the United States, including its territories, to another location within the United States; or (b) The U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States or its territories.

1.8 "**Domestic Communications Infrastructure**" or "**DCI**" means any Consolidated system that supports any communications originating or terminating in the United States, including its territories, including any transmission, switching, bridging, and routing equipment, and any associated software (with the exception of commercial-off-the-shelf ("COTS") software used for common business functions, e.g., Microsoft Office) used by, or on behalf of, Consolidated to provide, process, direct, control, supervise, or manage DC but would not include the systems of entities for which Consolidated has a contracted arrangement for interconnection, peering, roaming, long-distance, or wholesale network access.

1.9 "**Incident Response Plan**" means a written plan documenting Service Provider's policies, controls, procedures, and resources for identifying, responding to, mitigating, and recovering from Security Incidents, and the roles and responsibilities of its management, staff, and independent contractors in responding to Security Incidents.

1.10 "**Personal Data**" means information (regardless of form) that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a

particular individual or household, as may be further defined under Data Privacy Laws, and includes CPNI and information that constitutes "personal information," "personal data," "personally identifiable information," or any similarly defined term under Data Privacy Laws.

1.11 "**Personnel**" or "**Service Provider Personnel**" means (a) all employees, agents, contractors and/or subcontractors of Service Provider, and (b) all subcontractors' respective employees, agents and contractors who provide any portion of the Provided Services in connection with the Agreement, and (c) all of Service Provider's Subprocessors.

1.12 "**Principal Equipment**" means all telecommunications and information network equipment (e.g., hardware, software, platforms, operating systems, applications, protocols) that supports core telecommunications or information services, functions, or operations.

1.13 "**Provided Services**" means any and all products or services provided by Service Provider to Consolidated pursuant to the Agreement.

1.14 "**Security Incident**" means any actual or reasonably suspected (a) accidental or unauthorized access, acquisition, alteration, destruction, disclosure, loss, modification, processing, or storage of Consolidated Data; (b) activity that results in an unauthorized disruption or denial of Consolidated services, systems, or networks; or (c) unauthorized access or modification to Consolidated's systems or systems used to access, process, or store Consolidated Data or Consolidated's systems or networks.

1.15 "**U.S. Records**" means Consolidated customer billing records, customer/subscriber information, personally identifiable information, sensitive Personal Data (as defined by Data Privacy Laws), call detail records, internet protocol data records, Customer Proprietary Network Information, geolocation data, and any other information used, processed, or maintained in the ordinary course of business related to the services offered by Consolidated within the United States, including information subject to disclosure to a U.S. federal or state governmental entity under the procedures set forth in 18 U.S.C. § 2703(c), (d) and 18 U.S.C. § 2709.

2. Security Program Requirements. Without limiting any data security provisions in the Agreement, Service Provider shall implement and maintain a comprehensive documented information security program based on the NIST Standards contained in Publication 800-115, ISO 27001, or an equivalent standard ("**Security Program**") that implements and maintains industry best practices physical, administrative, and technical safeguards which protect the confidentiality, integrity, availability, and security of Consolidated Data, Consolidated**'s** systems and networks, and Service Provider's systems and networks with access to Consolidated Data and are designed to prevent Security Incidents ("**Security Measures**"). Such Security Program shall, at a minimum, comply with the requirements of Table 1 below, as applicable.

	Category	Description
(i)	**Risk and Vulnerability Management**	1. Conduct an information security risk assessment at least annually and whenever there is material change in Service Provider's business or technology practices, and document assessments. 2. Allow for Consolidated to periodically assess Service Provider's security posture via one or more of the following, at Consolidated's discretion: Consolidated's review of Service Provider's compliance and security documents; Service Provider's completion of a Consolidated-provided due diligence questionnaire; third-party assessment, or an audit of Service Provider by or on behalf of Consolidated. 3. Maintain a register or matrix of risks and mitigation steps taken to reduce probability and/or impact of risks. 4. Conduct continuous vulnerability assessments on systems where Consolidated Data is being hosted, stored, or processed. 5. Prioritize high risk vulnerabilities over lower risk ones.

		6. Address extreme risk accessing vulnerabilities such as zero-day flaws immediately upon discovery or notice. 7. Implement a process, either manual or automated, to monitor for security alerts. 8. Implement change management processes to ensure changes do not weaken or damage security controls or processes. 9. Maintain a patch management program. Implementation of patches must not exceed 90 days for high or medium severity patches as defined by the Common Vulnerability Scoring System (https://www.first.org/cvss/). 10. Service Provider must have an emergency patch process for critical patches that deploys patches as soon as possible.
(ii)	**Data Collection, Retention, and Disposal**	1. Limit Consolidated Data processed to what is needed in the provision of the Provided Services. 2. Prohibit storage of Consolidated Data on high-risk media outside Service Provider's physical or logical control such as portable media, staff personal devices, personal accounts, personal file sharing methods. 3. Implement appropriate Data Loss Prevention (DLP) controls to detect and prevent unauthorized removal of Consolidated Data from Service Provider's systems. 4. Securely and irreversibly dispose of Consolidated Data whether stored on systems or media. 5. Back up Consolidated Data when not on Consolidated managed systems. Backups must be transferred and stored offsite using strong encryption. 6. Allow for the return of Consolidated data to Consolidated within a reasonable period of time, at the request of Consolidated.
(iii)	**Data Inventory**	Maintain a current inventory of all Principal Equipment, hardware, software, cloud resources, and media used in the provision of the Provided Services.
(iv)	**Awareness and Training**	Ensure that personnel and subcontractors take security and privacy awareness training that addresses protecting the confidentiality, integrity and accessibility of Consolidated Data and systems, at least annually, and understand their roles and responsibilities. Service Provider Personnel that will interact with Consolidated customers should also take training in identity theft prevention.
(v)	**Subcontractor Oversight**	1. Only retain subcontractors pursuant to written agreements that include provisions equivalent to Service Provider's agreement with Consolidated, and that require subcontractors to maintain adequate safeguards that maintain the confidentiality, integrity, and availability of Consolidated Data. 2. Regularly assess and monitor subcontractors to confirm their compliance.
(vi)	**Access Controls**	1. Not share any Consolidated Data with any third parties except as permitted in the Agreement (MSA and/or SOW). 2. Limit access to Consolidated Data and systems to Service Provider Personnel in accordance with the principle of least privilege.

		3. Have a multi-factor authentication framework. 4. At least quarterly, audit access rights to ensure only those who require access are provisioned with it. 5. Strictly control privileged, administrator, or other elevated user access, and strictly forbid shared accounts to access Consolidated Data, especially as it pertains to accounts with elevated privilege. 6. Prevent terminated personnel or subcontractors from accessing Service Provider's systems and Consolidated Data by terminating their physical and electronic access to Consolidated Data promptly. 7. Service Provider Personnel access to Consolidated systems, networks, and data must be provided using a Consolidated managed device or Consolidated Virtual Desktop Infrastructure ("**VDI**"). 8. Service Provider must adhere to Consolidated's Service Provider Acceptable Use Policy in the Service Provider Code of Conduct when accessing Consolidated systems, networks, and data. 9. For mobile devices that may access Consolidated Data, impose centrally managed strong passcode, biometrics, inactivity lock, and a process to remotely wipe lost or stolen devices. 10. Service Provider is prohibited from storing Consolidated Data on publicly accessible internet storage locations such as cloud storage buckets without proper access controls.
(vii)	**User Authentication and Passwords**	1. Maintain security control over user IDs, passwords, and other authentication identifiers. 2. Require strong passwords including requirements for minimum password length, lockout, expiration period, complexity, reuse, encryption, changing of default passwords, and security communication of and usage of temporary passwords. 3. Block user access after multiple unsuccessful attempts to login. 4. Assign unique user identification and passwords. 5. Change all vendor supplied default passwords. 6. Protect passwords by salting and hashing or an equivalently secure alternate method prior to storage. Use cryptographically strong algorithms when hashing passwords. 7. Never allow hardcoding of passwords into scripts or software, even in pre-release versions of scripts or software. 8. Require all users accessing Service Provider's internal or hosted network remotely to use a secure method of connection using multifactor VPN or equivalent connection method. 9. If possible, restrict third party users to strictly those resources they need by using VDI. 10. Terminate user sessions after a predetermined period of inactivity.

(viii)	**Intrusion Detection and Response**	1. Maintain anomaly detection tools, relevant to Service Provider's systems which allow for reliable detection of anomalous events, which may include SIEM, IDS/IPS, malware detection, behavior-based detection, and other relevant tools. 2. Maintain current antivirus definitions and related updates to security detection tools to ensure up-to-date operation. 3. Maintain policies and procedures that accurately describe the incident response process including detect, respond, and recover processes.
(ix)	**Encryption**	1. Ensure strong encryption of Consolidated Data using cryptographically strong encryption algorithm including Consolidated Data in motion, at rest, and in backups. 2. Safeguard the confidentiality, integrity, and security of all encryption keys associated with Consolidated Data and maintain cryptographic and hashing algorithm types, strength, and key management process consistent with industry practices.
(x)	**Firewalls and Network Structure**	Implement firewalls with stable and secure code between the organization's information systems, the internet, and other public networks.
(xi)	**Segregation of Data**	1. Implement controls to ensure Consolidated Data is not comingled with any other Service Provider customer data. 2. Impose logical and physical segregation of development and testing environments from production environments. 3. Use mock data in development and testing environments.
(xii)	**Off-Premises Information Security**	1. Prohibit the storage, access, transportation, or use of Consolidated Data outside of the organization's security boundary or organization's remote access standards. 2. Prevent access from non-managed systems such as personal devices.
(xiii)	**Physical Security for Locations Accessing / Hosting Consolidated Data**	Maintain reasonable restrictions on physical access. 1. Implement clean desk policy, limit access to contractor personnel and authorized visitors, keep documents secured in locked office or file cabinet when not in use. 2. Lock workstations when unattended. Automatically lock workstations after reasonable inactivity. 3. Require visitors to prove identity, sign a visitor register, document reason for visit, person(s) visited and wear an identification badge for the duration of their stay. For Consolidated Data centers or similar facilities, visitors must be always escorted. 4. If the location hosts Consolidated Data and is not staffed 24x7, install alarms and entry point security cameras for off-hours access monitoring with recordings retained for at least thirty (30) days.

(xiv)	**Disaster Recovery / Business Continuity**	1. Maintain Disaster Recovery and Business Continuity policies and procedures. 2. Develop Business Continuity Plans for all systems involved with the provision of the Provided Services. 3. Perform annual disaster recovery tests for systems involved with the provision of the Provided Services.
(xv)	**Artificial Intelligence**	Without prior written approval from Consolidated, Service Provider should not use Consolidated Data to train AI models or on AI tools (either owned by the Service Provider or a third party); or use source code developed by external AI tools and resources.

3. Security Incident And Response.

3.1 Security Incident Response Plan. Service Provider shall implement and maintain an Incident Response Plan that enables Service Provider to (a) take actions to address any known or suspected Security Incident including ransomware, business email compromise, insider threat and data breach; (b) take appropriate remedial action; and (c) protect the confidentiality, integrity, and availability of Consolidated Data.

3.2 Notification of Security Incident. In the event of a Security Incident, Service Provider shall notify Consolidated without undue delay, and in no event later than forty-eight (48) hours after the initial detection of a Security Incident by contacting Consolidated's Cyber Incident Response Team at networksecurity@consolidated.com. Such notification shall include all information necessary for Consolidated to expeditiously respond to the incident and comply with applicable Law, including, to the extent possible, (a) a description of the Security Incident, including the suspected cause, the nature of the information affected, the categories and approximate number of Data Subjects affected, the categories and approximate number of records involved, and a description of the current and any anticipated impact, and the likely consequences thereof; (b) the expected resolution time (if it has not already been resolved); (c) attack vector, if known; (d) whether a forensics company was engaged (e) corrective measures to be taken, evaluation of alternatives, and next steps; and (f) the name and phone number of the Service Provider's Service Provider that Consolidated may contact to obtain further information and updates.

3.3 Response to Security Incident. At Service Providers sole expense, Service Provider will (a) activate its Incident Response Plan; (b) promptly investigate and determine the exposures that led to the Security Incident; (c) take all necessary steps to eliminate or contain the exposure and prevent further incidents; (d) collect, preserve, and document evidence regarding the Security Incident, in each case in sufficient detail to meet reasonable expectations of forensic admissibility; and (e) provide Consolidated with all information, logs, or images reasonably requested by Consolidated in connection with the Security Incident, including, but not limited to, all information to allow Consolidated and each Consolidated Affiliate to meet any obligations to report or inform of the Security Incident under Data Privacy Laws and assess the risk to Consolidated, or Consolidated Data, including Personal Data. Service Provider will promptly provide Consolidated with updated notifications as it becomes aware of additional material information and regularly keep Consolidated apprised of the status of the Security Incident and all matters related to it.

3.4 Cooperation. Service Provider shall cooperate with Consolidated's own response to and investigation of any Security Incident, and with any investigation relating to any Security Incident that is carried out by or at the direction of any government authority.

3.5 Security Incident Notification Decision. Service Provider acknowledges and agrees that it is Consolidated's decision whether and when to disclose a Security Incident to affected individuals or regulators in the absence of any laws or regulations requiring Service Provider to report or notify.

3.6 Public Statements. Service Provider shall not make any public statement about any Security Incident or Consolidated security vulnerability nor notify affected individuals of any Security Incident without Consolidated's prior written approval, unless Service Provider is required to do so pursuant to applicable Laws, in which case it shall provide Consolidated prior written notice of its intention to make such public statement or notify affected individuals.

3.7 Costs of Remediation of Security Incidents. In the event of any Information Security Incident arising out of or relating to any (a) breach or alleged breach by Service Provider or by any Service Provider Personnel of the representations, warranties or covenants contained in this Security Addendum; (b) any Information Security Incident; or (c) breach or alleged breach of Service Provider's obligations under this Security Addendum relating to privacy or security or caused by Service Provider's negligence or willful misconduct, Service Provider shall pay for or reimburse Consolidated for (i) expenses incurred to provide warning or notice to Consolidated's former and current employees, Service Providers, customers, and other persons and entities whose Personal Data or Confidential Information may have been disclosed or compromised as a result of the Security Incident (the "Affected Persons") and to law-enforcement agencies, regulatory bodies or other third parties as required to comply with law, or as otherwise directed by Consolidated; (ii) expenses incurred either directly by Consolidated or through Consolidated's retention of an independent third party forensic investigator, legal counsel, or any other third party, to investigate assess or remediate the Security Incident and to comply with applicable law and/or relevant industry standards; (iii) expenses related to the reasonably anticipated and commercially recognized consumer data breach mitigation efforts, including, but not limited to costs associated with the offering of credit monitoring for a period of at least twelve (12) months or such longer time as is required by law or recommended by one or more of Consolidated's regulators or any other similar protective measures designed to mitigate any damages to the Affected Persons; (iv) fines, penalties, or interest that Consolidated pays to any governmental or regulatory authority; (v) legal expenses incurred in connection with a Security Incident or to address any claims by third parties as a result of the Security Incident or investigation by law-enforcement agencies or regulatory bodies; and (vi) expenses incurred for the retention of a public relations or crisis management firm in order to manage communications on behalf of Consolidated related to any Security Incident.

4. Inspection And Audit Rights.

4.1 Documents. Service Provider shall establish and maintain complete and accurate records necessary to document compliance with this Security Addendum, including, without limitation, accounts of all transactions involving Consolidated Data, and shall retain such records in accordance with the terms of the Agreement.

4.2 Audits by Consolidated. Upon at least thirty (30) days' prior notice to Service Provider, Service Provider shall permit Consolidated, its auditors, designated Service Provider and regulators, to audit and inspect, at Consolidated's expense, and no more often than once per year (unless otherwise required by Consolidated regulators or applicable laws, or unless a previous inspection revealed any deficiency); (i) the Service Provider's facilities where Consolidated Data is stored or maintained by or on behalf of Service Provider; (ii) the Service Provider's systems used to share, disseminate, or handle Consolidated Data; (iii) Service Provider's security practices and procedures to Processing Consolidated Data; and (iv) records required to be retained by Service Provider under this Agreement.

4.3 Third-Party Audits. Service Provider shall, at its own cost and expense annually undergo an AICPA compliant System and Organization Controls (SOC) audit of its organization and systems related to and the provision of the Provided Services, which shall be completed by an independent third-party accounting firm. Upon request from Consolidated, Service Provider shall promptly provide its most current SOC report(s) to Consolidated, as well as any mitigation, remediation, or corrective action plans for any high and medium assessed risk.

4.4 Security Assessments. Service Provider shall, at its own cost and expense, cooperate with Consolidated to assess Service Provider's compliance with this Security Addendum and the Agreement. Service Provider shall provide Consolidated or Consolidated's third-party auditors and examiners with access to Service Provider's systems, facilities, records, policies, and personnel related to and the provision of the Provided Services to aid such assessment and to demonstrate Service Provider's compliance. Upon the completion of any such assessment, should Consolidated inform Service Provider of weaknesses or deficiencies where Service Provider's security systems or controls do not meet the requirements of this Security Addendum or the Agreement, or applicable Law, Service Provider shall promptly implement measures it will take to remedy such deficiencies and notify Consolidated in writing when those measures are implemented.

5. Insurance.

5.1 General. Service Provider shall maintain insurance coverages and amounts in accordance with the requirements set out in the Agreement.

5.2 Cyber Insurance. In addition, Service Provider shall secure and maintain cyber liability insurance, including coverage for business interruption, with limits for both first-party and third-party claims of at least 10 Million Dollars each, in the aggregate. Consolidated shall be added as an additional insured under any cyber liability insurance policy obtained by Service Provider.

6. High-Risk Country List. Unless otherwise agreed to in writing by Consolidated, Service Provider is prohibited from using Service Provider Personnel, services, networks or assets located in a high-risk country* as indicated on the list below ("**High-Risk Country**") in the provision of the Provided Services. *If a region of a given country is specified, only that region is prohibited and not the entire country.

Country	Region(s)		Country	Region(s)		Country	Region(s)
Afghanistan	All		Honduras	All		Pakistan	All
Algeria	All		Hong Kong	All		Philippines	Sulu Archipelago, Mindanao
Belarus	All		India	State of Jammu, Kashmir		Russia	All
Bolivia	All		Indonesia	All		Saudi Arabia	All
Burkina Faso	All		Iran	All		Somalia	All
Burundi	All		Iraq	All		South Sudan	All
Cambodia	All		Israel	All		Sudan	All
Central African Republic	All		Kenya	All		Somalia	All
Chad	All		Lebanon	All		Syria	All
China	All		Libya	All		Tajikistan	All
Colombia	All		Mali	All		Tanzania	All
Congo	All		Mauritania	All		Tunisia	All
Crimea	All		Moldova	All		Turkey	Near Syria / Iraq Borders
Cuba	All		Mongolia	All		Turkmenistan	All
Ecuador	All		Myanmar	All		Uganda	
El Salvador	All		Nicaragua	All		Ukraine	All
Eritrea	All		Niger	All		United Arab Emirates	All
Guinea-Bissau	All		Nigeria	All		Venezuela	All
Haiti	All		North Korea	All		Yemen	All
						Zimbabwe	All

7. Breach. A breach of this Security Addendum is a material breach of the Agreement.

8. Notifications.

8.1. Notifications of a Security Incident should be sent to networksecurity@consolidated.com using the subject line: Security Breach.

8.2. Notifications of a concern related to Security Measures should be sent to networksecurity@consolidated.com using the subject line: Vendor Security Concerns.

9. Relationship to the Agreement.

9.1. The parties agree that this Security Addendum replaces and supersedes any existing or prior Security Addendum to which Service Provider may have been subject.
9.2. Except as expressly modified herein, the terms of the Agreement shall remain in full force and effect.
9.3. To the extent of any conflict or inconsistency between this Security Addendum and any other document comprised within the Agreement, the order of precedence shall be, each when applicable, in descending order: 1) this Security Addendum, 2) the Data Privacy Addendum, 3) the FCC Addendum, 4) the amended master agreement, and 5) any Order or SOW.
9.4. Under no circumstances shall an Order or SOW modify this Security Addendum, unless such modification specifically references the term it is overriding and the document containing such modification is signed by both parties.
9.5. This Security Addendum will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement.

10. Term. The term of this Security Addendum shall begin on the last date signed below and will end upon the termination of the Agreement.

11. General Provisions. Should any provision of this Security Addendum be invalid or unenforceable, then the remainder of this Security Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (a) amended as necessary to ensure its validity and enforceability, while preserving the intent of the provision as closely as possible; or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein. Unless otherwise expressly stated herein, the parties will provide notices under this Security Addendum in accordance with the Agreement.

Signed: Consolidated Communications	**Service Provider: _____**
By: _____	By: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
Date: _____	Date: _____