Information Security Requirements Appendix

June 30, 2026

Lumen Information Security Requirements Appendix

This Information Security Requirements Appendix ("Appendix") applies whenever a Supplier Processes or has physical or logical access to Lumen Confidential or Highly Confidential Information or has access to a Lumen Information System or Facility. If any requirements in this Appendix conflict with the terms of any Agreement, Data Protection Addendum, or Data Security Addendum between the parties, the provisions more protective of Confidential or Highly Confidential Information will prevail. Capitalized terms used but not defined in this Appendix will have the same meanings as in the Agreement.

Definitions

- ***Affiliate,*** if not defined in the Agreement, with respect to either party, shall mean any entity that is directly or indirectly in control of, controlled by, or under common control with such party whether now existing, or subsequently created or acquired during the term of the Agreement.
- ***Confidential Information,*** if not defined in the Agreement, means (i) any Personal Information or Sensitive Personal Information (ii) Customer Proprietary Network Information (CPNI), as defined at 47 USC § 222(h), (iii) Lumen Data, (iv) Highly Confidential Information, (V) and other sensitive, proprietary or legally-protected data Lumen owns, controls, collects, discloses or otherwise makes available.
- ***Agreement,*** means any contract or agreement Data Protection Addendum, Data Security Addendum, Statement of Work (SoW), Order or Purchase Order governing Supplier's provision of services and/or deliverables to Lumen.
- ***Lumen,*** means Lumen Technologies Service Group, LLC, its Affiliates, and operating units.
- ***Information System(s),*** means any networks, applications, computers, media, software, hardware, and mobile devices used to Process Lumen Confidential or Highly Confidential Information or logically connect to such Systems.
- ***Highly Confidential Information,*** means non-public financial or revenue data, Intellectual Property (IP) and trade secrets, merger or acquisition activities, Controlled Unclassified Information (CUI), network diagrams containing critical infrastructure information, and any other information that is designated as "Highly Confidential" or similar, or that a reasonable person would understand to be highly confidential given its nature or the circumstances of disclosure.
- ***Highly Privileged Accounts (HPAs),*** are accounts with system level administrative or super-user access to devices, applications or databases; administration of accounts and passwords on a system; or ability to override system or application controls.
- ***Lumen Data,*** means any data, information or material (i) provided to Supplier by or on behalf of Lumen or otherwise input into Supplier's software or portal by or on behalf of Lumen ("Lumen Provided Data"), or (ii) generated by Supplier's software based on Lumen Provided Data and received by Lumen during the course of using Supplier's software.
- ***Personal Information,*** means information relating to an identified or identifiable natural person, and an identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to their physical,

physiological, mental, economic, cultural or social identity or information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

- ***Process or Processing,*** means to perform any operations upon Data (including but not limited to Lumen Confidential or Highly Confidential Information), whether or not by automatic means, including, but not limited to, collecting, recording, organizing, storing, adapting or altering, retrieving, accessing, consulting, using, disclosing by transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing, or destroying.
- ***Information Security Incident,*** is any actual or suspected event in which Lumen Confidential or Highly Confidential Information is or may have been lost, stolen, accessed, transferred, copied, altered, destroyed, disclosed, or used without authorization or in any manner not permitted under the Agreement or this Appendix.
- ***Security Standards,*** means the most secure and protective of (i) the security requirements of this Appendix; (ii) measures required by applicable law or industry standard; or (iii) relevant security measures considered best practices to protect the confidentiality, integrity and availability of Information and the Systems that Process it.
- ***Sensitive Personal Information,*** means social security numbers, credit card or financial account numbers, credit scores, driver's license or state ID numbers, health and wellness data, any Personal Health Information (as defined under HIPAA and its implementing regulations, including 45 C.F.R. Parts 160 and 164), login credentials, or any other Personal Information that (i) is deemed sensitive under applicable privacy laws , (ii) requires breach notification under applicable law, or (iii) which Lumen identifies as sensitive, whether pertaining to personal, business or employment activities of Lumen employees or customers.
- ***Supplier,*** is the entity that is a party to the Agreement and any Affiliate, subcontractor, subprocessor, or agent of such entity that Processes or has access to Lumen Confidential or Highly Confidential Information or has access to a Lumen Information System.
- ***Supplier Personnel,*** means Supplier's employees, and employees of its Affiliates, suppliers, subcontractors, subprocessors, and agents.

Security Requirements

1. Supplier will comply with this Appendix at all times when it accesses, stores or Processes Lumen Confidential or Highly Confidential Information. Supplier will maintain and adhere to written safety and facility procedures, data security procedures and other safeguards to prevent an Information Security Incident or any other unauthorized access to, use or alteration of Lumen Confidential or Highly Confidential Information, and such procedures will reflect best practices for information security. Supplier agrees to cooperate in good faith to modify its business practices to accommodate any future changes in the parties' hardware, software, or services, or in legal or industry standards regarding Lumen Confidential or Highly Confidential Information treatment that may affect reasonableness or effectiveness of the protections under this Agreement.
2. Before providing access to any Lumen Confidential or Highly Confidential Information, Supplier must obligate its Personnel, subcontractors and subprocessors with access to

Lumen Confidential or Highly Confidential Information to protect it in accordance with the confidentiality, data protection and security requirements in the Agreement, , and this Appendix and to verify such compliance through an appropriate due diligence process and flow-down obligations with respect to Supplier's subcontractors and subprocessors. Supplier shall take reasonable steps to ensure continuing compliance by its Personnel, subcontractors and subprocessors with this Appendix and shall remain responsible for their compliance.

3. Supplier shall terminate Supplier Personnel access to Lumen Confidential or Highly Confidential Information, whether physical or logical, no later than the date of Supplier Personnel separation or transfer to a role no longer requiring access to Lumen Confidential or Highly Confidential Information. Where Supplier Personnel have been assigned Lumen Single Sign-On (SSO) credentials, Supplier must notify Lumen of any such separation or transfer no later than the day of that event.
4. Supplier Personnel with access to Lumen Confidential or Highly Confidential Information must participate in mandatory information security awareness training provided by the Supplier before obtaining access to Lumen Confidential or Highly Confidential Information, and on at least an annual basis while they have access to Lumen Confidential or Highly Confidential Information.
5. Unless prohibited by applicable law, Supplier shall notify Lumen promptly and act only upon instruction from Lumen concerning any request by a third party, including without limitation law enforcement, governmental authority, or in connection with litigation or other legal process for Lumen Confidential or Highly Confidential Information disclosure or for information concerning Lumen Confidential or Highly Confidential Information Processing in connection with the Agreement including any request received from an individual concerning any Personal Information as part of a data subject request .
6. Supplier shall not Process Lumen Confidential or Highly Confidential Information on personal accounts, including individual email or cloud services accounts (e.g., Gmail, Yahoo, Dropbox, Google Drive), or on personally owned computers, devices, or media.
7. Supplier will not Process Lumen Confidential or Highly Confidential Information beyond what is strictly necessary to perform the Supplier Services under the Agreement.
8. Supplier will securely erase Lumen Confidential or Highly Confidential Information from all media using current commercially reasonable erasure methods before Supplier reuses or provides any third party with media on which Lumen Confidential or Highly Confidential Information has been Processed.
9. Supplier must receive Lumen approval before (a) moving Lumen Confidential or Highly Confidential Information from its Lumen-approved hosting jurisdiction to a different hosting jurisdiction; or (b) provisioning remote access to such Lumen Confidential or Highly Confidential Information from any location other than the Lumen-approved hosting jurisdiction or other Lumen-approved jurisdiction, or (c) moving Lumen Confidential or Highly Confidential Information from its Lumen-approved physical location or jurisdiction to a different physical location or jurisdiction.
10. Suppliers must not implement or use remote, out-of-band, or hardware-level access mechanisms, including remote KVM technologies (e.g., tools that emulate direct

keyboard, video, or mouse access) to access Lumen Systems or Information unless explicitly approved in writing by Lumen Global Security Services (GSS).

11. Supplier will not Process any Lumen Confidential or Highly Confidential Information at any location outside the United States, or through entities not incorporated or organized in the United States, without prior written consent from Lumen.
12. Supplier must implement encryption in any of the following instances:
    - When Lumen Confidential or Highly Confidential Information is at rest on portable computing and storage devices including, but not limited to:
        - Laptops
        - Tablets
        - Personal digital assistants
        - Diskettes
        - Mobile phones
        - USB flash drives
        - CDs
    - When transferring Lumen Confidential or Highly Confidential Information over public networks (such as the Internet) or over non-US soil
    - When Lumen Highly Confidential information is at rest and in transit

    Where encryption is required, Supplier must maintain cryptographic and hashing algorithm types, strength, and key management processes consistent with highly regarded industry practices. Any encryption required hereunder must be FIPS 140-2 validated/compliant.
13. Supplier Information Systems must have security controls that can prevent and detect attacks and must be continuously monitored. For example, network layer firewalls and intrusion detection/prevention Systems (IDS/IPS) between the internet and demilitarized zone (DMZ), and between DMZ and internal servers containing Lumen Confidential or Highly Confidential Information. Supplier must respond to IDS/IPS high and critical priority alerts as soon as reasonably practicable but in no case more than 72 hours.
14. Supplier must use at least a two-factor authentication method to authenticate any Supplier Personnel remotely accessing Supplier Information Systems and Supplier must secure such transmissions using industry standard encryption.
15. Supplier must use an auditable process (e.g., certification of destruction) to securely remove Lumen Confidential or Highly Confidential Information from Supplier Information Systems before disposal or re-use in a manner that ensures Lumen Confidential or Highly Confidential Information is not accessible or readable.
16. Supplier must ensure Supplier Information Systems are free from all malicious software (malware). Supplier must install and run anti-malware software on all Supplier Information Systems capable of running such software and must configure anti-malware software to automatically detect and remove harmful or malicious code. Supplier must configure the anti-malware software to update automatically and continuously to ensure definitions will never be more than 24 hours old.

17. Supplier will comply with Lumen *Drug Testing and Background Check* requirements available on the *Doing Business with Lumen* page.
18. Supplier shall comply with Lumen *Physical Security Administration Standards for Suppliers* available at the *Doing Business with Lumen* page.
19. Unless otherwise expressly agreed in the Agreement, development and testing environments must not contain Lumen Confidential or Highly Confidential Information, and any that are dedicated to Lumen Confidential or Highly Confidential Information shall only go "live" upon Lumen Global Security Services' review and approval.
20. Supplier must keep any back-up media containing Lumen Confidential or Highly Confidential Information stored at Supplier's site in a secure location (e.g., locked office or locked file cabinet), and Supplier must encrypt backup media using a standard consistent with industry practice. If off-site media storage is used, Supplier must have a media check-in/check-out process with locked storage for transportation. Supplier must give back-up information the same level of physical and environmental protection as the level of control applied at the main site.
21. Network layer security devices must allow only authorized connections and Supplier must review rule sets semi-annually at a minimum.
22. Mobile devices used to Process Lumen Confidential or Highly Confidential Information (including emails) must have strong mobile device security controls, including required passcode, minimum passcode length, inactivity lock, and a process in place to immediately and remotely wipe lost or stolen devices.
23. Supplier will not use Mobile Devices to Process Lumen Confidential or Highly Confidential Information absent a business need to perform under this Agreement. If so needed, Mobile Devices that contain Lumen Confidential or Highly Confidential Information will interact with or store Lumen Confidential or Highly Confidential Information only in an encrypted form using a strong cryptographic protocol with highly regarded, secure protocols consistent with commercially reasonable practices in Supplier's business sector.
24. Supplier must keep all software used in Supplier Information Systems current, and in no event must software be more than one version behind the current version in any system that Processes Lumen Confidential Information. Supplier shall develop, deploy, update, and maintain all Supplier software in strict accordance with relevant industry standards.

Additional Security Requirements for Sensitive Personal Information or Highly Confidential Information

In the event Supplier will or may Process Lumen Sensitive Personal Information or Highly Confidential Information, Supplier shall implement and maintain, in addition to the above Security Requirements, the following additional measures and controls:

1. Supplier must perform vulnerability assessments on Supplier Information Systems at least annually. For Supplier Information Systems that are internet-facing, Supplier must engage an independent external party to perform a vulnerability assessment and shall remediate as required in Audits.
2. Supplier must have or implement hardening and configuration requirements consistent with highest level industry practices, including testing and implementing all applicable

security-related fixes, command scripts, etc. provided by Operating System Vendors, User associations, and other trusted Third Parties in a time frame appropriate with the associated risk.

3. Supplier must have or implement appropriate data loss prevention (DLP) controls (e.g., disabling of universal serial bus (USB) ports, enabling DLP software, enabling uniform resource locator (URL)/Web filtering) to detect and prevent unauthorized removal of Lumen Confidential or Highly Confidential Information from Supplier Information Systems.
4. Supplier must implement processes to support the secure creation, modification, and deletion of Highly Privileged Accounts (HPAs). Supplier must review and update access rights at least quarterly for HPAs. Supplier must continually review HPA usage logs. Supplier must establish all HPA access using encrypted mechanisms (e.g., secure shell).
5. Supplier must monitor, record, and control physical access with physical access rights reviewed at minimum annually. Supplier must store physical access logs detailing access for a one (1) year period unless prohibited by local law. If not staffed 24x7, Supplier must install alarms and entry point security cameras for off-hours access monitoring and retain recordings for at least thirty (30) days.

Compliance

1. Supplier represents and warrants that it shall comply with all applicable laws and regulations applicable to Supplier's activities concerning Lumen Confidential or Highly Confidential Information governed by this Appendix, including, without limitation, all legal obligations concerning collection, use, disclosure, transfer, and Processing of Personal Information.
2. If Supplier Processes payment card information on behalf of Lumen, Supplier will comply with the current Payment Card Industry Data Security Standard (PCI-DSS), as amended or updated from time to time. Supplier will validate compliance with PCI-DSS, as needed, to permit Lumen to meet its compliance obligations, and will provide Lumen annually with a PCI-DSS compliance certificate signed by an officer of Supplier with oversight responsibility. If Supplier Processes financial account information (e.g., bank or credit union accounts), it will protect information in accordance with the National Automated Clearing House Association's NACHA/ACH Rules and Operating Guidelines. Supplier will provide Lumen annually with a NACHA/ACH compliance certificate, signed by an officer of Supplier with oversight responsibility.
3. If Supplier Processes any Lumen Confidential or Highly Confidential Information that includes Protected Health Information (PHI), it shall comply with Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Business Associate Agreement (BAA) located on the Doing Business with Lumen page.
4. If Supplier Processes any Lumen Confidential or Highly Confidential Information that includes banking or financial information, it shall comply with the U.S. Sarbanes-Oxley Act (SOX), the U.S. Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), the Federal Financial Institutions Examination Council (FFIEC) guidance, and the European Union's Digital Operations Resilience Act (DORA).

5. If Supplier Processes any Personal Information or Personal Data subject to the EU General Data Protection Regulation (GDPR) (Regulation 2016/679), the California Consumer Protection Act (CCPA), or any similar privacy or data protection laws, it shall comply with the Data Protection Addendum attached or incorporated into the Agreement, or if none, the Lumen Supplier Data Protection Addendum located on the Doing Business with Lumen page.
6. If there are additional legal or industry standards applicable to Supplier's Processing of Lumen Confidential or Highly Confidential Information, Supplier agrees to cooperate with Lumen to comply with such requirements, including, without limitation:
    - Execution of additional agreements and/or representations required to enable Lumen to comply with applicable law and/or compliance standards. Such documents may include, but are not limited to, Federal Acquisition Regulation (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), NIST SP 800-171 checklist items, or similar documents. Such provisions would be applicable to Suppliers providing commercial products, services, software, and off-the-shelf items
    - Implementation of additional or revised security controls required by applicable law or compliance standard
    - Completion of regulatory filings or compliance certifications applicable to Supplier
    - Completion of required regulatory or compliance audits
7. Unless and except to the extent expressly provided in the Agreement, Supplier must, in each case, seek and obtain prior written approval from Lumen regarding the scope of any Personal Information collected directly by Supplier from an Individual, as well as any notices provided, and any consent language used when collecting such information. In the case Supplier collects Personal Information directly from Individuals, Supplier shall comply with applicable data privacy laws and regulations, including those concerning notice, consent, access, and correction/deletion.

Information Security Incident

1. Supplier must develop and maintain an up-to-date incident management plan to promptly identify, prevent, investigate, and mitigate any Information Security Incidents and perform any required recovery actions to remedy the impact.
2. Supplier must log Information Security Incidents on Supplier's Information Systems and review (on a periodic basis (minimum quarterly)), secure, and maintain the logs for a minimum of twelve (12) months.
3. Supplier will promptly (but in no event later than 24 hours after discovery) inform Lumen in writing on becoming aware of any known or suspected Information Security Incident and provide any Incident-related Information and logs Lumen requests within the same timeframe.
4. Supplier shall report any Information Security Incidents to Lumen UNIcall at 1-866-864-2255 or at such contact information communicated to Supplier from time to time. Supplier will provide specific information on what Lumen Confidential or Highly Confidential Information was involved and any other information Lumen reasonably may request concerning the Information Security Incident details as soon as such information can be collected or otherwise becomes available and any remediation efforts undertaken

and will thereafter provide regular and timely updates throughout the ongoing investigation and remediation.

The parties will work cooperatively to secure the return or recovery of any Lumen Confidential or Highly Confidential Information as necessary. When Supplier experiences an information Security Incident, upon reasonable request of Lumen, Lumen may require Supplier to hire an independent, third-party forensic or security firm to assist with their investigation or remediation effort. Supplier will advise Lumen on the investigation results. Each party will work cooperatively with the other party on remediation and law enforcement activities, as appropriate.

5. Notwithstanding and excluded from any limitations in the Agreement, Supplier shall pay for or reimburse Lumen for all costs associated with an Information Security Incident, including, without limitation:
   - Forensic assessments
   - Breach notices
   - Credit monitoring or other fraud alert services
   - Regulatory investigations
   - Third-party audits
   - All other remedies either required by applicable law and regulation or which are required to remediate the Information Security Incident and prevent similar Information Security Incidents in the future
6. If requested by Lumen, and at the direction of Lumen, Supplier shall send breach notices regarding an Information Security Incident. Unless prohibited by applicable law or regulation, Supplier shall provide Lumen with reasonable notice of, and the opportunity to comment on and approve, the content of such breach notices before any publication or communication thereof to any third party. However, Lumen shall not have the right to reject any content in a breach notice that is specifically required to comply with applicable law or regulation. Should Lumen elect to send a breach notice regarding an Information Security Incident, Supplier shall provide all reasonable and timely information relating to the content and distribution of that breach notice as permitted by applicable law or regulation.
7. Other than approved breach notices, or to law enforcement or as otherwise required by law or regulation, Supplier may not make or permit any public statements concerning Lumen involvement with any such Information Security Incident to any Third Party without explicit written authorization from Legal and Public Policy (Legal).

Audits

1. Supplier shall monitor its security program effectiveness by conducting (or engaging a Third Party to conduct) audits and risk assessments of Supplier Information Systems against the requirements of written policies and procedures maintained as required by this Appendix and applicable law no less frequently than every twelve (12) months. Supplier shall be responsible for ensuring consistency of its security operations, including proactively monitoring and mitigating all vulnerabilities across any Supplier Information Systems used to access or Process Lumen Confidential or Highly Confidential Information or Lumen Information Systems.

2. Upon request from Lumen, Supplier will provide information to Lumen to enable Lumen to determine compliance with this Appendix. As part of the Lumen assessment of Supplier's internal control structure, Lumen may require Supplier to, without limitation, answer security questionnaires or conduct server, database, and other network hardware scans and submit an attestation by an officer of Supplier with knowledge of Supplier's compliance.
3. Upon request, Supplier must provide to Lumen reports of any audits and assessments conducted on Supplier Information Systems, which reports shall include, at a minimum, the audit and/or assessment scope and any vulnerabilities, issues, findings, concerns, and/or recommendations to the extent that they impact Lumen Confidential or Highly Confidential Information. Both parties shall treat such reports provided by Supplier to Lumen as Lumen Highly Confidential Information.
4. Supplier must remediate within thirty (30) days any items rated as high or critical (or similar rating indicating similar risk) in any Supplier Information Systems audits or assessments. Lumen reserves the right to request remediation completion in less than 30 days, compensating control implementation, or suspension of further activity where necessary to adequately protect Lumen Confidential or Highly Confidential Information.
5. Upon request, with reasonable advance notice and conducted in such a manner not to unduly interfere with Supplier's operations, Lumen reserves the right to conduct, or to engage Third Parties to conduct, an audit of Supplier's compliance with the requirements in this Appendix relating to Lumen Confidential or Highly Confidential Information including but not limited to:
    - A review of Supplier's applicable policies, processes, and procedures
    - A review of the results of Supplier's most recent vulnerability assessment (e.g., application vulnerability scanning, penetration testing, and similar testing results) and accompanying remediation plans
    - A review of contract documentation for Supplier's subcontractors and subprocessors with access to Lumen Confidential or Highly Confidential Information to ensure such documentation contains all appropriate flow-down clauses
    - On-site assessments of Supplier's physical security arrangements and Supplier Information Systems during Supplier's regular working hours pursuant to a mutually agreeable audit plan
6. Lumen reserves the right to conduct an onsite audit of Supplier on ten (10) business days prior written notice during regular business hours. This right shall survive termination or expiration of the Agreement so long as Supplier Processes Lumen Confidential or Highly Confidential Information provided under the Agreement. Supplier agrees to cooperate fully with Lumen or its designee during such audits and shall provide access to facilities, appropriate resources, and applicable supporting documentation.
7. If Lumen has a reasonable basis to believe the Supplier has breached or is likely to breach the terms of this Appendix, Lumen may, upon five (5) days' notice, perform a vulnerability assessment, which assessment will be in addition to any assessment in the ordinary course. At reasonable request from Lumen, Supplier will promptly cooperate with Lumen to develop a plan to protect Lumen Confidential or Highly Confidential Information from any applicable failures or attacks, which plan will include prioritization of recovery efforts

and identification, and creation of implementation plans for alternative data centers or other storage sites and backup capabilities.

Material Breach

1. Notwithstanding anything to the contrary herein or in the Agreement, Supplier's (including Supplier Personnel) failure to comply with the obligations set forth in this Appendix also constitutes a material breach of the Agreement, with such rights and remedies set forth therein or under applicable law and regulation.
2. Lumen or the applicable Lumen Affiliate owning any Lumen Confidential or Highly Confidential Information accessed pursuant to the Agreement may enforce the terms of this Appendix as permitted or required by applicable law and regulation.

Miscellaneous

1. Lumen may collect Personal Information of Supplier Personnel, which may be stored in databases located and accessible globally and used it as needed under with the performance of the Agreement, Lumen will be the Controller (as that term is defined in applicable data protection laws) of Personal Information of Supplier Personnel and will use reasonable technical and organizational measures to ensure such Personal Information is Processed in conformity with applicable data protection laws.