Information Security Requirements Appendix

October 23, 2020

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

Definitions

- ***Affiliate,*** if not defined in the Contract Document, 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 Contract Document.
- ***Confidential Information*****,** means information defined as confidential in the Contract Document and includes (i) any 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 his 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; (ii) Customer Proprietary Network Information (CPNI), as defined at 47 USC § 222(h); (iii) any types of data or information specifically identified in this Appendix, and (iv) any other sensitive, proprietary or legally-protected data that is owned, controlled, collected, disclosed or otherwise made available by Lumen.
- ***Contract Document,*** as used in this Appendix, means any contract, agreement, statement of work, task order or purchase order governing the provision of services and/or deliverables by Supplier to Lumen.
- ***Lumen,*** means Lumen Technologies, Inc., its Affiliates and operating units.
- ***Information System(s),*** means any networks, applications, computers, media, software, hardware, and mobile devices that are used to Process Lumen Confidential Information or that logically connect to such systems.
- ***Highly Privileged Accounts, or 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.
- ***Process or Processing,*** means to perform any operation or set of operations upon data (including but not limited to Lumen 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.
- ***Security Incident,*** is any actual or suspected event in which Lumen 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 Contract Document 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 Confidential Information,*** means Lumen Confidential Information that involves Social Security Numbers, credit cards, any other financial account numbers, health and wellness data, customer data, login credentials, any data deemed sensitive under applicable law, any data that meets the definition of any breach notification requirement under applicable law, or other Confidential Information which Lumen identifies as Sensitive Confidential Information, whether any of the the foregoing information pertains to personal, business or employment activities.
- ***Supplier,*** is the entity that is a party to the Contract Document and any Affiliate, subcontractor, or agent of such entity that Processes or has access to Lumen Confidential Information or has access to an Information System.

- ***Supplier Personnel,*** means Supplier's employees, as well as its Affiliates, suppliers, subcontractors, and agents and their respective employees.

Security Requirements

1. Supplier will, at all times that it accesses, stores or Processes Lumen Confidential Information comply with this Appendix. Supplier will maintain and adhere to written safety and facility procedures, data security procedures and other safeguards to prevent a Security Incident or any other unauthorized access to, use or alteration of Lumen 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 the treatment of Lumen Confidential Information that may affect the reasonableness or effectiveness of the protections under this Agreement.
2. Prior to providing access to any Lumen Confidential Information, Supplier must obligate Supplier Personnel to comply with the security required in the Contract Document and this Appendix and verify such compliance through an appropriate due diligence process. Supplier shall take reasonable steps to ensure continuing compliance by such Supplier Personnel with this Appendix and shall remain responsible at all times for their compliance.
3. Supplier shall undertake all reasonable measures to terminate Supplier Personnel access to Lumen Confidential Information, whether physical or logical, no later than the date of personnel separation or personnel transfer to a role no longer requiring access to Lumen 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 Information must participate in mandatory information security awareness training provided by the Supplier prior to obtaining access to Lumen Confidential Information and thereafter on at least an annual basis while such personnel have access to Lumen 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 disclosure of Lumen Confidential Information or for information concerning the Processing of Lumen Confidential Information in connection with the Contract Document or this Appendix, including any request received from an individual concerning their information that may be Lumen Confidential Information.
6. Lumen Confidential Information shall not be Processed on personal accounts (e.g., 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 Information beyond what is strictly necessary to perform the Supplier services under the Contract Document.
8. Supplier will securely erase Lumen Confidential Information from all media, using then current commercially-reasonable erasure means, before Supplier reuses or provides any third party with media on which Lumen Confidential Information has been Processed.
9. Supplier must receive approval from Lumen prior to (a) moving Lumen Confidential Information from its Lumen-approved hosting jurisdiction to a different hosting jurisdiction; or (b) provisioning remote access to such Lumen Confidential Information from any location other than the Lumen-approved hosting jurisdiction or other Lumen-approved jurisdiction or (c) moving Lumen Confidential Information from its Lumen-approved physical location or jurisdiction to a different physical location or jurisdiction.
10. Supplier will not Process any Lumen Confidential Information at any location outside the United States or through entities that are not incorporated or organized in the United States without prior written consent from Lumen.

11. Encryption must be implemented in any of the following instances: (a) portable computing and storage devices such as laptops, tablets, personal digital assistants, diskettes, mobile phones, USB flash drives, CDs, and portable hard drives (collectively referred to as "Mobile Devices")containing Lumen Confidential Information must be encrypted at rest; (b) transferring Lumen Confidential Information over public networks (such as the Internet) or over non-US soil; and (c) Lumen Highly Confidential information must be encrypted 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 certified/compliant.
12. Supplier Information Systems must have security controls that can detect and prevent attacks and must be continuously monitored. For example, network layer firewalls and intrusion detection/prevention Systems (IDS/IPS) between the Internet and DMZ, and between DMZ and internal servers containing Lumen Confidential Information. IDS/IPS high and critical priority alerts must be responded to as soon as reasonably practicable but in no case more than 72 hours.
13. Any Supplier Personnel remotely accessing Supplier Information Systems must be authenticated using at least a two-factor authentication method and such transmissions must be secured using industry standard encryption.
14. Supplier must use an auditable process (e.g., certification of destruction) to remove Lumen Confidential Information from Supplier Information Systems prior to disposal or re-use in a manner that ensures that the Lumen Confidential Information may not be accessed or readable.
15. Supplier must ensure that Supplier Information Systems are free from all malicious software (malware). Anti-malware software must be installed and running on all Supplier Information Systems capable of running such software, and it must be configured to automatically detect and remove harmful or malicious code. The anti-malware software must be configured to update automatically and continuously to ensure the definitions will never be more than 24 hours old.
16. Supplier will comply with Lumen Drug Testing and Background Check requirements available on the Doing Business with Lumen portal.
17. Supplier shall comply with Lumen Physical Security Administration Standards available at the Supplier Portal.
18. Unless otherwise expressly agreed in the Contract Document, development and testing environments must not contain Lumen Confidential Information and any that are dedicated to Lumen Confidential Information shall only go "live" upon Lumen Global Security's review and approval, as appropriate.
19. Any back-up media containing Lumen Confidential Information stored at Supplier's site must be kept in a secure location (e.g., locked office or locked file cabinet) and be encrypted to 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. Back-up information must be given the same level of physical and environmental protection as the level of control applied at the main site.
20. Network layer security devices must allow only authorized connections and rule sets must be reviewed at minimum semi-annually.
21. Mobile devices used to Process Lumen 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 remotely wipe lost or stolen devices.
22. Supplier will not use Mobile Devices to Process Lumen Confidential Information absent a business need to perform under this Agreement. If so needed, Mobile Devices that contain Lumen Confidential Information will interact with or store Lumen 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. Mobile Devices used to Process Lumen 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 remotely wipe lost or stolen devices.

23. All software used in Supplier Information Systems must be kept current and in no event be more than one version behind the current version in any significant Processing system. All Supplier software shall be developed, deployed, updated, and maintained in strict accordance with relevant industry standards.

Additional Security Requirements

In the event Supplier will or may Process Lumen Sensitive 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, to include 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 USB ports, DLP software, URL/Web filtering) to detect and prevent unauthorized removal of Lumen Confidential Information from Supplier Information Systems.
4. Supplier must implement processes to support the secure creation, modification, and deletion HPAs. Supplier must review and update access rights at least quarterly for HPAs. HPA usage logs must be continually reviewed. All HPA access must be established using encrypted mechanisms (e.g., secure shell).
5. Physical access must be monitored, recorded and controlled with physical access rights reviewed at minimum annually. Physical access logs detailing access must be stored for a period of one (1) year unless prohibited by local law. If not staffed 24x7, alarms and entry point security cameras must be installed for off-hours access monitoring with recordings retained 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 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 Standards (PCI-DSS), as amended or updated from time to time. Supplier will validate compliance with Payment Card Industry Data Security Standards, 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 that 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 Information that includes Protected Health Information (PHI), it shall comply with HIPAA and the Business Associate Agreement located on the Doing Business with Lumen page.
4. If Supplier Processes any Lumen Confidential Information that includes banking or financial information, it shall comply with the U.S. Sarbanes-Oxley Act, the U.S. Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), and the Federal Financial Institutions Examination Council (FFIEC) guidance.
5. If Supplier Processes any Lumen Confidential Information that includes personal information or personal data subject to the EU General Data Protection Regulation (Regulation 2016/679), the California Consumer

Protection Act, or any similar privacy or data protection laws, it shall comply with the Lumen Data Processing Agreement located on the Doing Business with Lumen portal.

6. In the event there are additional legal or industry standards applicable to Supplier's Processing of Lumen Confidential Information, Supplier agrees to cooperate with Lumen to comply with such requirements, including, without limitation: (a) execution of additional agreements required by applicable law or compliance standard; (b) implementation of additional or revised security controls required by applicable law or compliance standard; (c) completion of regulatory filings or compliance certifications applicable to Supplier; and (d) completion of required regulatory or compliance audits.
7. Unless and except to the extent expressly provided in the Contract Document, Supplier must, in each case, seek and obtain prior written approval from Lumen regarding the scope of any Confidential Information to be collected directly by Supplier from an individual, as well as any notices to be provided and any consent language to be used when collecting such information. In the case of Confidential Information collected directly from individuals by Supplier, Supplier shall comply with applicable data privacy laws and regulations, including those concerning notice, consent, access and correction/deletion.

Security Incident

1. Supplier must develop and maintain an up-to-date incident management plan to promptly identify, prevent, investigate, and mitigate any Security Incidents and perform any required recovery actions to remedy the impact.
2. Security Incidents on Supplier's Information Systems must be logged, reviewed on a periodic basis (minimum quarterly), secured, and maintained 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 Security Incident.
4. Supplier shall report any Security Incidents to Lumen UNIcall at 1-866-864-2255 or at such contact information communicated to Supplier from time to time. In any such instance, Supplier will give specific information on what Confidential Information was involved and any other information Lumen reasonably may request concerning the details of the Security Incident, 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 Confidential Information as necessary. When Supplier experiences the incident, upon reasonable request of the Lumen, Supplier may be required to hire an independent, third party forensic or security firm to assist with this investigation or remediation effort. Supplier will advise Lumen of the final results of the investigation. 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 Contract Document, Supplier shall pay for or reimburse Lumen for all costs associated with a Security Incident, including, without limitation, costs of forensic assessments, breach notices, credit monitoring or other fraud alert services, regulatory investigations, third party audits, and all other remedies either required by applicable law and regulation or which are required to remediate the Security Incident and prevent similar Security Incidents in the future.
6. If requested by Lumen, and at the direction of Lumen, Supplier shall send breach notices regarding a 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 prior to any publication or communication thereof to any third party, except 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 a 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 Security Incident to any third-party without the explicit written authorization of the Lumen Legal Department.

Audits

1. Supplier shall monitor the effectiveness of its security program 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 proactive monitoring and mitigation of all vulnerabilities across any Supplier Information Systems used to access or Process Lumen 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 scans of servers, databases and other network hardware, 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 scope of the audit and/or assessment and any vulnerabilities, issues, findings, concerns, and/or recommendations in so far as they impact Lumen Confidential Information. Such reports provided by Supplier to Lumen shall be treated as confidential.
4. Supplier must remediate within thirty (30) days any items rated as high or critical (or similar rating indicating similar risk) in any audits or assessments of Supplier Information Systems. Lumen reserves the right to request remediation to be completed in less than 30 days, implementation of a compensating control, or suspension of further activity where necessary to adequately protect Lumen 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 Information including but not limited to: (a) a review of Supplier's applicable policies, processes, and procedures, (b) 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, and (c) 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. 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 Contract Document so long as Supplier Processes Lumen Confidential Information provided under the Contract Document. 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 to Lumen.
6. If Lumen has a reasonable basis to believe that 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 Information from any applicable failures or attacks, which plan will include prioritization of recovery efforts, identification of and 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 Contract Document, Supplier's (including Supplier Personnel) failure to comply with the obligations set forth in this Appendix also constitutes a material breach of the Contract Document, with such rights and remedies set forth therein or under applicable law and regulation.
2. Lumen or the applicable Lumen Affiliate owning any of the Lumen Confidential Information being accessed pursuant to the Contract Document may enforce the terms of this Appendix as permitted or required by applicable law and regulation.

Miscellaneous

1. Supplier understands and agrees that Lumen or its Affiliates may require Supplier to provide certain personal information such as the name, address, telephone number, and e-mail address of Supplier's representatives in transactions to facilitate the performance of the Contract Document, and that Lumen, its Affiliates, and its contractors may store such data in databases located and accessible globally by their personnel and use it for necessary purposes in connection with the performance of the Contract Document, including but not limited to Supplier payment administration. Lumen or the applicable Lumen Affiliate will be the controller of this data for legal purposes and agrees to use reasonable technical and organizational measures to ensure that such information is processed in conformity with applicable data protection laws.