LOUISIANA-PACIFIC CORPORATION
DATA SECURITY ADDENDUM
(CANADA)

TABLE OF CONTENTS

1. **Definitions.** All capitalized terms not defined herein have the meaning set forth in the Agreement.

1.1. "Agreement" means the applicable agreement between Service Provider and Company pursuant to which Service Provider is providing its Services.

1.2. "Anti-Virus Signatures" means a catalog of data that describes the current Malicious Software threats (e.g., virus, worms, spyware) and how Anti-Virus Software is to detect and remove the threat from the given system, message, or file.

1.3. "Anti-Virus Software" means an industry-standard software specifically written to prevent the introduction or intrusion of Malicious Software through a set of Anti-Virus Signatures.

1.4. "Collect" means to make a forensic copy of the data and storing such data in a secure location.

1.5. "Company" means Louisiana-Pacific Corporation, together with its affiliates and subsidiaries.

1.6. "Company Data" means all Company Personal Data, data, information, visual or graphic representations and other similar materials in any medium or format electronic, tangible or otherwise and which are provided to or accessed by Service Provider or any of its Affiliates or any of their Subcontractors by or at the direction of Company or which Service Provider or its Affiliates or any of their Subcontractors create, collect, process, store, generate or transmit in connection with the provision of the Services or the performance of Service Provider's obligations under the Agreement. Company Data shall be considered and treated as Company's Confidential Information.

1.7. "Company Personal Data" means data and/or information that Service Provider or any of its Affiliates or any of its or their Subcontractors may obtain or have access to, Process or transmit in connection with the Agreement or any SOW which consists of information or data naming or identifying a natural Person, including but not limited to: (a) information that is explicitly defined as a regulated category of data under any Data Privacy Laws applicable to Company; (b) non-public personal information, including but not limited to a business or personal email address, employee identification number, address, military identification number or other military records, phone numbers, vehicle registration plate number, IP address, national identification number, passport number, TSA Number, social security number or social insurance number (in whole or part), or driver's license number; (c) health or medical information, such as insurance information, medical prognosis, diagnosis information or genetic information; (d) financial information, such as a policy number, Payment Information, credit history, financial account number, or any code or password that would permit access to a financial account; (e) sensitive personal data, such as name, date of birth, mother's maiden name, race, marital status, gender or sexuality, background check information, judicial data such as criminal records, or Internet protocol addresses relating to use of websites or assigned to a person; (f) biometric data; and/or (g) genetic data. Company Personal Data shall be considered and treated as Confidential Information.

1.8. "Company Systems" means the networks, equipment, hardware, software and communications systems and components and elements thereof owned, used, or operated by Company.

1.9. "Data Privacy Laws" means laws relating to data privacy, trans-border data flow or data protection, including but not limited to: the California Consumer Privacy Act and California Privacy Rights Act; the Colorado Privacy Act; the Connecticut Data Privacy Act; the Utah Consumer Privacy Act; the Virginia Consumer Data Protection Act; the federal Gramm-Leach-Bliley Act; the European Union General Data Protection Regulation, known as GDPR (including nation-specific rules or laws promulgated under GDPR by European Union member states) ; the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada; all rules, regulations and binding enforcement actions promulgated by the United States Federal Trade Commission; any and all amendments, successor or supplemental laws relating to any of the foregoing; and any additional laws or regulations that may be promulgated in the future in any applicable jurisdiction.

1.10. "End User(s)" means any individual Company permits to use the Services, which may include, without limitation, employees, agents, contractors, consultants, outsourcers, supplies or other individuals (including third parties).

1.11. "Governmental Authority" means each federal, state, provincial and municipal government, authority and agency and its respective agencies, departments, authorities, and commissions.

1.12. "Information Security Incident" means: (a) the attempted or actual unauthorized acquisition, access, use, Processing, loss, or disclosure of Confidential Information; (b) the suspicion or reasonable belief that there has been an attempted or actual unauthorized acquisition, access, use, Processing, loss, or disclosure of Confidential Information; or (c) the unauthorized use or attempted use of any Service Provider Systems to gain access to any Company System.

1.13. "Malicious Software" means any type of software or program which is designed to: (a) cause unauthorized access to or intrusion upon; or (b) otherwise disrupt and/or damage, computer equipment, software, and/or data, including but not limited to viruses, worms, Trojan horses, spyware, ransomware, or other software intended to cause system crashes, network packet floods, unauthorized use of system privileges, unauthorized access to sensitive data or execution of malicious code that destroys data.

1.14. "PA DSS Requirements" means the Payment Application Data Security Standard maintained by the PCI which applies to Persons that process payment card transactions with participating major payment card networks.

1.15. "Payment Information" means the payment card (credit, debit, or gift card) information collected from a Person, including the cardholder's name and billing address, the payment card number and the expiration date, PIN or PIN block, magnetic strip data, information relating to a payment card transaction that is identifiable with a specific account, and the external verification (e.g., CVV2) code for the payment card.

1.16. "PCI" means the Payment Card Industry Security Standards Council and its successors.

1.17. "PCI DSS Requirements" means the Payment Card Industry Data Security Standard maintained by the PCI which applies to Persons that process payment card transactions with the participating major payment card networks.

1.18. "Person" means any natural person, corporation, partnership, limited liability company, trust, association, firm, entity, or Governmental Authority.

1.19. "Physical Media" means electronic storage media and tangible material used to store Company Data, including but not limited to external hard drives, USBs in all forms, tapes (reel, cassette), cartridges, disks, drums, CDs, DVDs, paper, microfilm, and microfiche.

1.20. "Process" or "Processing" means any operation or set of operations performed or to be performed with respect to or in connection with Company Personal Data, whether or not by automatic means, such as creating, capturing, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, transmitting, transferring, disclosing, or destroying Company Personal Data.

1.21. "Service Provider" means the entity engaged by Company to provide Services under one or more Agreements.

1.22. "Subcontractor" means any subcontractor of Service Provider providing services as permitted under the Agreement.

1.23. "Service Provider Systems" means the equipment, software and communications systems and components used, supplied and/or developed by Service Provider or any of its Affiliates or Subcontractors for the provision of the Services, including, without limitation any payment card gateways or card processors.

1.24. "Workstation(s)" means all laptop(s), notebook(s), desktop(s), tablet(s), mobile device(s), and any other computer(s) (thin client, physical or virtual), used by Service Provider in providing the Services or otherwise Processing Company Confidential Information.

2. **Application and Technological Advances**. The Parties understand and agree that technologies and practices evolve over time, and that the administrative, physical, technical, and organizational measures and controls set forth in this Data Security Addendum may be subject to progress and development. In that regard, Service Provider, Affiliates of Service Provider, and Service Provider Personnel may, in some cases and upon the prior written approval of Company, implement alternative but equivalent (or functionally superior) measures to those set forth in this Data Security Addendum; provided, however, that the implementation of such alternatives do not result in any degradation or reduction of the effectiveness of the associated measures and controls; and further provided, Company's approval of the same shall not be deemed a waiver of any of Service Provider's obligations under this Data Security Addendum. Service Provider will be liable and indemnify Company for any failure of Affiliates of Service Provider and Service Provider Personnel to comply with the terms and conditions of this Data Security Addendum to the same extent as if such failure was attributable to Service Provider itself. Company may request, and Service Provider shall not unreasonably refuse to enter into, a written undertaking to protect Company's confidentiality and systems security in case of physical or on-line access to Company's premises and/or systems.

3. **Service Provider Safeguarding Obligations**. Service Provider will develop, maintain, and implement a comprehensive written information security program that complies with applicable Data Privacy Laws, including mandatory training to Service Provider Personnel who have access to Company Confidential Information regarding the privacy, confidentiality and information security requirements set forth in the Agreement and this Data Security Addendum. Service Provider's information security program and the information security programs of its Affiliates and all Subcontractors will include appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to: (a) ensure the security and confidentiality of Company Confidential Information; (b) protect against any anticipated threats or hazards to the security and integrity of Company Confidential Information and (c) protect against any Information Security Incident.

4. **Security Standards**. Service Provider will, and, as applicable, will cause Service Provider's Affiliates and Subcontractors to, at all times maintain (or any applicable successor certifications or reports accepted by Company):

   a. an ISO/IEC ISO 27001certification (the "ISO Certification"); or
   b. An annual Service Organization Control ("SOC") 2 Type II report (the "SOC 2") ; or
   c. if available, a SOC 3 report (the "SOC 3") (the SOC 1, SOC 2, and SOC 3 collectively, the "SOC Reports"); or
   d. an NIST SP 800-53 Revision 5 certification (the "NIST Certification").

   SOC 2 reports shall be prepared in accordance with the SSAE19 reporting standard or higher. SOC 2 and SOC 3 reports shall fully cover the security, availability, integrity, confidentiality, and privacy-related controls of the information systems (including procedures, people, software, data, and infrastructure) that are used by Service Provider and its Affiliates and Subcontractors in processing Company Data. Service Provider will and will cause Affiliates of Service Provider and Subcontractors to promptly provide a copy of the SOC, ISO or NIST Certification report to Company upon execution of the Agreement and in no event later than thirty (30) days of receipt from the independent auditor for each annual period in which Service Provider, Affiliate

of Service Provider, or Subcontractor receives the same. Service Provider will promptly notify Company of any deficiencies identified in any reports. Service Provider will promptly address and resolve any such deficiencies to the extent necessary to comply with Service Provider's obligations under the Agreement and the Schedule 1 (Security) and notify Company when any such deficiency is resolved. If any deficiency is not promptly resolved, it will be deemed a material breach of the Agreement by Service Provider.

5. **Penetration Testing**. Service Provider, where confidential information, infrastructure services or application development are provided to Company, will engage, at its own costs, an independent third party to conduct penetration testing on a yearly basis, including human manual testing (i.e., not just automated vulnerability scanning), to evaluate the security controls of the Service Provider Systems, Software Program, application, host and network layers used to provide the Services following industry standard methodologies (e.g. OWASP and OSSTMM). At Service Provider's own costs, Service Provider will, and will cause its Affiliates and Subcontractors to, document how they will protect all Company Confidential Information discovered during testing. Service Provider shall provide Company with copies of its report at the time they are available and in no event later than thirty (30) days after receipt for each annual period. Service Provider will, and will cause its Affiliates and Subcontractors to, use a Rules of Engagement (ROE) document for clear expectations on penetration test timing, escalation procedures, scope, communications method, and any other reasonably related elements, and provide to Company for its approval prior to conducting penetration testing. Service Provider will promptly notify Company of any deficiencies identified as well as corrective actions necessary for all vulnerabilities to be corrected. Should any critical weakness be identified, Service Provider will, and will cause its Affiliates and Subcontractors (as applicable) to, undertake corrective actions within seven (7) calendar days of receipt of the report. Should any high weakness be identified, corrective actions shall be undertaken by Service Provider, its Affiliates, or Subcontractors (as applicable) within thirty (30) calendar days of receipt of the report. At Service Provider's own costs, Service Provider will, and will cause its Affiliates and Subcontractors to, retest any high weaknesses and provide Company tangible evidence that such weaknesses have been remediated to the reasonable satisfaction of Company. Company will not be liable for any failure, negative impact, system degradation, product failure or system failure related to Service Providers Systems due to compliance under this Section 5.

6. **Credentials and End User Authentication**. Service Provider will ensure, and will cause Affiliates of Service Provider and Subcontractors to ensure, that each End User is assigned a unique User ID and password, token, or biometric identifier ("Credentials"), along with a secondary factor for authentication (Multi-Factor Authentication). This will allow End Users to access the Services only after authentication with valid multi-factor credentials. Credentials will be stored at rest using a one-way hashing algorithm (SHA-256, or the equivalent), and will be encrypted whenever transmitted over the Internet in accordance with the data encryption requirements set forth in Section 20. Upon authentication, the Services will provide the ability to track each End User's activity through the use of a unique session identifier associated with the Credentials and each login session.

7. **Passwords or Passwordless Authentication**. All passwords, whether manually created by the End User or automatically generated must comply with minimum complexity requirements including, without limitation, a requirement that all passwords have a minimum of twelve (12) alpha numeric characters and include letters, special characters, and numbers. All Service Provider Systems and Workstations will: (a) contain password history controls to prohibit use of the three (3) most recently used passwords; (b) require a verification question before resetting password; (c) not log passwords under any circumstances; (d) encrypt passwords in storage and transmission; and (e) have controls in place to force a password to expire after a defined period of time but at least within 90 days (all of the foregoing, the **"Password Security Requirements"**). In no instance will Service Provider Personnel manually select and assign a password to an End User of any Services. Any automatically generated passwords for the Services will be: (i) automatically generated in a manner which produces a random value; (ii) delivered automatically via email to the requesting End User; and (iii) valid only for one successful login, requiring the receiving End User to manually select a replacement password upon login with the automatically generated password. Passwordless authentication is acceptable, as long as two factors for authentication are applied (certificates, SMS, application provisioning of 6-digit PINs, etc.)

8. **ID and Access Management**. The Services shall have the ability to use identity and access management standards such as: (a) SCIM and/or make API integration available for the creation, modification, and deletion of End User accounts and access permissions, and the exchange of identity data; and (b) identity and access management standards such as SAML, OAuth, OpenID Connect in order to make authentication and authorization decisions.

9. **Application Security**. The Services and the Service Provider Systems will provide, where applicable, configurable security controls including, at a minimum: (a) the ability to revoke access to the Services after a defined number of consecutive failed login attempts ("**Lockout**"); (b) the ability to specify the Lockout time period; (c) the ability to specify the number of invalid login requests before initiating the Lockout; (d) compliance with the Password Security Requirements; (e) controls to terminate an End User session after a defined period of inactivity; (f) the ability to accept logins to the Services from only certain IP address ranges; (g) the ability to restrict logins to the Services to specific time periods; (h) the ability to delegate End User authentication or federate authentication via SAML; and (i) up-to-date, via automation or a centrally controlled process, application and operating system patches and services packs.

10. **Access to Company Systems**. Service Provider acknowledges that Company retains the right to terminate Service Provider access to all or some of the Company Systems at any time, in its sole discretion without any liability. If Service Provider is provided remote access to the Company Systems Service Provider must comply with all of the applicable security requirements set forth herein. Additionally, Service Provider, its Affiliates, employees, Subcontractors and agents shall ensure that all inbound and outbound remote access to and from Company Systems and any systems that Process, transmit or store Company Personal Data utilize an end-to-end encryption method in accordance with the data encryption requirements set forth in Section 20.

11. **Service Provider System Security and Workstations**. Any facilities containing the Service Provider Systems will, at a minimum: (a) be structurally designed to withstand adverse weather and other reasonably predictable natural conditions; (b) implement appropriate physical environmental safeguards to protect systems from damage related to smoke, heat, cold, water, fire, humidity, or fluctuations in electrical power; (c) be supported by uninterruptible power supplies and on-site backup power generating systems; (d) implement appropriate controls to ensure that only authorized personnel are allowed physical access to the facility; (e) use industry standard processes to dispose of physical components containing Company Confidential Information; and (f) utilize, at minimum, WPA2 for all wireless network security. The Service Provider System will maintain firewalls at all logical demilitarized zones and internet connection points and include safeguards designed to prevent possible bridging of Company Systems with non-Company networks, including the prevention of logical connectivity from Service Provider Systems to non-Company networks (e.g., the internet) while simultaneously connected to Company Systems (e.g., "split tunneling" VPNs). Any Workstations that Service Provider uses to access Company's Confidential Information will: (i) be documented and tracked in a formal asset management system; (ii) utilize encrypted hard drives; (iii) have an installed and functional software-based firewall; (iv) ensure operating system are within vendor support and applications and operating systems have all critical patches installed within one (1) weeks; (v) accept only passwords that comply with the Password Security Requirements; and (vi) have a screen saver or other method of lockout that activates after no more than fifteen (15) minutes of inactivity.

12. **Physical Media**.

12.1 General. Service Provider will use best efforts to only transfer Company Data electronically using methods that comply with this Data Security Addendum. If Service Provider determines that the Company Data cannot securely be sent electronically, Service Provider will inform Company and obtain Company's consent to transport the Company Data using Physical Media. All transport of Physical Media containing Company Data must comply with this Section 12.

12.2. Inventory and Chain of Custody. Service Provider will have a single point of contact responsible for creating and maintaining an inventory of Physical Media and periodically auditing the accuracy of the inventory. The inventory must include, at minimum, a tracking or other identification number associated with any shipment of Physical Media and indicate whether any Physical Media received was placed into storage, returned, destroyed, or erased. Service Provider will update the inventory upon the receipt, transport, or disposal of Physical Media. All Physical Media containing Company Data must be stored in a locked room or cabinet with access limited to personnel with a need to access such areas to carry out job responsibilities. Service Provider must maintain a fully documented chain of custody, tracking all handling and removal of Physical Media, that includes, at minimum, the condition of the Physical Media at the time of access or removal, the identification of the handler, purpose, date, time, intended disposition, and expected return date if applicable.

12.3. Packaging and Transport. If Company consents to the transport of Company Data using Physical Media, all Physical Media must be encrypted according to industry standard best practices that incorporate, at minimum, the data encryption practices set forth in Section 20 prior to transport. Prior to transporting Physical Media, Service Provider will contact the Company individual responsible for receipt to confirm date/time of transport and after delivery obtain written confirmation of receipt of the Physical Media from recipient. The outside of any container holding Physical Media must be addressed to a specific recipient by name and at a business address. No other marking or identifying information should be marked on the container. At minimum the following will be required when transporting Physical Media: (a) Physical Media will not be transported through a major distribution hub and will not be mass handled or undergo automated sorting; (b) point to point monitoring (e.g., signatures designating any change of custody – sender, courier or receiver, bar code scanning, delivery control numbers, logging); (c) GPS tracking; and (d) shipping manifests that include shipper, receiver, and driver signatures with delivery time and pick-up. In no event will Service Provider permit Physical Media to be left unattended or in an unsecured vehicle.

13. **Production System Reliability.** Service Provider will ensure, and will cause Affiliates of Service Provider and Subcontractors to ensure, as applicable, that all networking components, SSL accelerators, load balancers, web servers, application servers, database servers, and storage devices used to provide the Services are configured using accepted industry-standard redundant design methodology, including, at a minimum: (a) web and database server clustering and load balancing; (b) file system and database mirroring, replication, or other equivalent technologies; and (c) carrier-class disk storage using RAID disks and multiple data paths.

14. **Backup and Data Recovery Procedures.** Service Provider will: (a) ensure that Company Confidential Information is backed up, encrypted, and stored in a location and format available for retrieval as needed up to the last committed transaction; (b) store copies of Company Confidential Information and data recovery procedures in a different place from where the primary computer equipment processing the Company Confidential Information is located; (c) have specific procedures in place governing creation of and access to copies of Company Confidential Information; (d) review data recovery procedures at least every six (6) months; and (e) maintain a log of all restoration efforts, the description of the restored data, the Person responsible for restoration, and which data (if any) required manual input during the data recovery process.

15. **Disaster Recovery and Business Continuity.** Service Provider currently has and will maintain at all times an appropriate disaster recovery, business continuity and contingency plan and related policies and procedures (collectively, the "**DR Plan**") agreed upon by Service Provider and Company in writing and will furnish a summary of its DR Plan to Company in writing upon execution of this Data Security Addendum. The DR Plan will provide for continued operation in the event of a catastrophic event affecting Service Provider's business operations and will be in accordance with internationally accepted business continuity, contingency and disaster recovery planning standards, procedures and practices, including, but not limited or restricted to the following minimum requirements: (a) a disaster recovery facility that is geographically remote from its primary data center, along with all required hardware, software, and Internet connectivity sufficient to provide the Services without substantial reduction or degradation of functionality or availability, in the event the primary data center were to be rendered unavailable; (b) secure backup copies of the Company Confidential Information that is not stored on a Company System; (c) restoration of the Services within twelve (12) hours after Service Provider's declaration of a disaster; and (d) maximum data loss of four (4) hours. Service Provider will notify Company as soon as possible after it deems a service outage to be a disaster and will address any such outage in accordance with the terms of its DR Plan. Service Provider will test all features of its DR Plan at least once per calendar year and will provide the results of such tests to Company upon request.

16. **Logging.** The Service Provider Systems, Workstations used in performing the Services will provide, where applicable, the following minimum logging capabilities and/or features: (a) enabled, active, and configured firewalls, routers, network switches, servers, workstations and operating systems with logging capabilities to record event records in sufficient detail to the respective default logging destination or to a centralized syslog server (for network systems) for diagnostic and analytical purposes in the event of an Information Security Incident; (b) recorded access log entries containing, at a minimum, the date, time, User ID, URL requested or entity ID operated on, operation performed (viewed, edited, etc.) and source IP address; and (c) the ability to track certain administrative changes to the Service Provider Systems, Workstations used in performing the Services (such as password changes and adding custom fields) in a "Setup Audit Log" (all of the foregoing, the "**Log Records**"). All Log Records must be made available for viewing, download, and local storage by Company and maintained for a minimum of two (2) years in a physically and logically secured location. Service Provider will, and will cause Affiliates of Service Provider and Service Provider Personnel to, upon request, provide to Company copies of any Log Records.

17. **Intrusion Detection and Prevention.** Service Provider will monitor the Services and the Service Provider Systems for unauthorized access, interception, or interruption using accepted industry-standard network-based intrusion detection and prevention mechanisms.

18. **Malicious Software; Virus Protection.** Service Provider and, as applicable, Affiliates of Service Provider and Subcontractors will install and maintain on all Workstations and Service Provider Systems Anti-Virus Software (including anti-malware and endpoint protection features) that uses real time protection features maintained in accordance with the Anti-Virus Software vendor's recommended practices. In addition, Service Provider will ensure and, as applicable, will cause Affiliates of Service Provider and Subcontractors to ensure that: (a) the Anti-Virus Software checks for new Anti-Virus signatures at least daily; and (b) the Anti-Virus Signatures are current. Service Provider will and, as applicable, cause Affiliates of Service Provider and Service Provider Personnel to immediately remove any Malicious Software discovered or which may be present in the Service Provider Systems, Workstations or within the Services. All Services will, where applicable, perform real-time scanning on files and other data uploaded into the applicable Services to identify and eliminate any files or other data containing Malicious Software.

19. **No Disabling Devices**. Neither the Services nor the Service Provider Systems will utilize or otherwise introduce or permit any software routines or elements capable of causing or enabling unauthorized access to, disabling, deactivating, deleting or otherwise damaging or interfering with any Company Systems.

20. **Data Encryption.** Service Provider will, and as applicable, will cause Affiliates of Service Provider and Subcontractors to implement and utilize industry standard best practices that incorporate at a minimum, 256-bit VeriSign SSL Certification and minimum 2048-bit RSA public keys to protect Company Confidential Information, including during transmissions between Company's network and the Service Provider Systems. Company Confidential Information and any backups of Company Confidential Information at rest will be encrypted according to industry standard best practices that incorporate, at minimum Advanced Encryption Standard (AES) disk encryption with a minimum key length of 128 bits. All portable devices, including, without limitation, smart phones, and tablet devices, containing or accessing Company Confidential Information must utilize end-to-end encryption for transmissions from the portable device and all data at rest stored or accessed from the device.

21. **System Audits.** At any time after the first anniversary of the effective date, Company may elect to conduct a data security audit, with at least ten business days' prior notice to Service Provider, to benchmark Service Provider's then-current data security practices against the best practices of leading providers of services that are the same as or similar to Services provided by Service Provider. If any such audit reveals that the data security practices and processes then utilized by Service Provider are materially inconsistent with industry best practice, or do not comply with the obligations required hereunder, then Service Provider will reimburse Company for the cost of such audit and Company and Service Provider will promptly establish and implement a plan to implement identified best practices into the Services. Company will not be liable for any failure, negative impact, system degradation, product failure or system failure related to Service Provider's systems due to compliance under this Section 21.

22. **Right to Monitor.** Company will have the right to monitor Service Provider's compliance with this Data Security Addendum. During normal business hours, and without prior notice, Company or its respective authorized representatives may inspect Service Provider's facilities and equipment, and any information or materials in Service Provider's possession, custody, or control, relating in any way to Service Provider's obligations under the Agreement or this Data Security Addendum. An inspection performed pursuant to this Data Security Addendum will not unreasonably interfere with the normal conduct of Service Provider's business. Service Provider will cooperate fully with any such inspection initiated by Company. Service Provider will respond promptly and appropriately to any inquiries from Company relating to the Processing of Company Personal Data.

23. **Subcontractors.** Service Provider will perform sufficient due diligence prior to the retention of any Subcontractor to ensure that such Subcontractor will not, in any way, compromise the security, confidentiality, availability or integrity of any Company Confidential Information. Further, Service Provider will ensure that the terms of its subcontract with any Subcontractor are consistent with the responsibilities and obligations of the Agreement and this Data Security Addendum. Service Provider will take appropriate action to cause its Affiliates and Service Provider Personnel to be advised of and comply with the applicable terms and conditions of the Agreement and will ensure that Service Provider Personnel are trained regarding their handling of Company Confidential Information and the associated obligations under this Agreement.

24. **Access to Confidential Information.** Service Provider will ensure that any Service Provider Personnel that has access to Company Confidential Information will be granted such access based on a least privilege approach/need to know principle. Service Provider will also maintain policies that prohibit Service Provider, Service Provider Affiliates, or Service Provider Personnel from using personally owned Workstations for the processing of Company Confidential Information. Service Provider will not remove Company Confidential Information from its location or otherwise copy Company Confidential Information unless that removal or retention is reasonably necessary to perform the Services. Company Confidential Information must always be anonymized/obfuscated before transfer to non-live environments.

25. **Rights to Company Data.** Company Data is and will at all times remain the property of Company. Service Provider hereby waives any and all statutory and common law liens it may now or hereafter have with respect to Company Data. Service Provider will ensure that all Company Data will be kept strictly separated from Service Provider's data and data of any other client by appropriate technical means. Without limiting the generality of any obligations under the Agreement or this Data Security Addendum, Service Provider shall not use or permit use of the Company Data to market or solicit any business for any of Service Provider's, or its Affiliates', products, or services or those of any Service Provider Personnel, or otherwise use Company Data for any purpose other than to perform the Services under the Agreement. Unless expressly agreed to by Company in writing, neither Service Provider, nor its Affiliates or Service Provider Personnel shall have the right to aggregate Company Data or use, sell, creative derivative works from, or otherwise exploit any aggregated Company Data.

26. **Development and Vulnerability Management.** For any software development processes related to the provision of Services under the Agreement, Service Provider must address common coding vulnerabilities by: (a) using secure coding guidelines and latest leading industry-accepted practices for vulnerability management such as the Open Web Application Security Project (OWASP) Guide, the SANS CWE Top 25 Most Dangerous Software Errors, and CERT Secure Coding; and (b) training Contractor Personnel responsible for developing the software to be provided as part of the Services at least annually in up-to-date secure coding techniques, including, but not limited to, how to avoid common coding vulnerabilities. Service Provider shall have in place a comprehensive vulnerability management program for the regular (minimum monthly) identification, categorization, and timely remediation of technical and process vulnerabilities at the infrastructure and application layers of the Service Provider System(s) provided. Software patches to correct vulnerabilities must be installed and activated within the following timeframes:

Severity	CVSS Score	Remediation Requirement
Critical	9.0 or higher	<= 1 week
High	7.0 to 8.9	<=30 days
Medium	4.0 to 6.9	<=60 days
Low	0.1 to 3.9	<=90 days

27. PCI Compliance.

27.1. PCI Compliance Documentation. If Service Provider is providing payment processing services or the Services include payment processing functionality, Service Provider represents and warrants that Service Provider: (a) is presently compliant with all applicable PCI DSS Requirements and PA DSS Requirements; (b) has registered as a service provider with all required entities (e.g., Visa, MasterCard, etc.); (c) to the extent required by the PCI DSS Requirements and/or the PA DSS Requirements (i.e., after reaching appropriate transaction thresholds) has undergone an assessment against PCI DSS Requirements and PA DSS Requirements performed by an independent Qualified Security Assessor (a "**QSA**") within

the last twelve (12) months; (d) maintains a current, compliant Attestation of Compliance certificate, a report of validation, a report on compliance and any exceptions noted therein (collectively, the "**Compliance Documentation**"), under PCI DSS Requirements; and (e) will make the Compliance Documentation available for Company's review upon request.

27.2. PCI Non-Compliance Event. Service Provider covenants and agrees to be and remain in compliance with all applicable PCI DSS Requirements and PA DSS Requirements and to perform the necessary steps to validate its compliance with PCI DSS Requirements and PA DSS Requirements and shall notify Company immediately in the event of any of the following (individually, a "**Non-Compliance Event**"): (a) Service Provider learns or has reason to believe that it is no longer in compliance with PCI DSS Requirements and/or PA DSS Requirements; or (b) Service Provider undergoes an adverse change in its certification or compliance status with respect to PCI DSS Requirements and/or PA DSS Requirements. Upon the occurrence of a Non-Compliance Event, Service Provider will immediately provide Company with a detailed plan to remediate such Non-Compliance Event. In the event Service Provider cannot provide, after reasonable prior notice from Company, validation of its compliance with PCI DSS Requirements and/or PA DSS Requirements and the necessary Compliance Documentation as required under the Agreement, Company shall have the right to engage a QSA to conduct an audit of Service Provider to determine Service Provider's compliance with PCI DSS Requirements and PA DSS Requirements, and Service Provider shall pay all costs of such an audit. Any such audit shall be conducted by a QSA on behalf of Company and shall be conducted so as to reasonably minimize any disruption to Service Provider's operations. Service Provider shall reasonably cooperate with such QSA, including providing reasonable access to its facilities and applicable personnel necessary to audit and test compliance. Service Provider shall implement any remediation measures recommended by such QSA as soon as reasonably possible in order either to remain certified as compliant with PCI DSS Requirements and PA DSS Requirements or to re-obtain certification under PCI DSS Requirements or PA DSS Requirements and shall provide a detailed plan with respect to any recommended remediation measures. Service Provider acknowledges that it is solely responsible at all times for the security of any Payment Information or cardholder data in transit, at rest or in its possession. A failure of Service Provider to maintain certification of its compliance with PCI DSS Requirements and/or PA DSS Requirements shall be considered a material breach of the Agreement by Service Provider.

27.3. Investigation of PCI Information Security Incident. In the event of an Information Security Incident and in addition to other obligations arising from such Information Security Event, Service Provider shall provide full access to PCI members and/or PCI-approved entities so that such Information Security Incident may be thoroughly investigated without restriction. Service Provider shall maintain the security of any Payment Information provided to Service Provider for the duration of the Agreement and for the life of the Payment Information after the expiration or earlier termination of the Agreement. Service Provider agrees to incorporate best practices security in its software to prevent the interception of transaction data, including Payment Information.

28. **Authority to Process Company Personal Data.** Service Provider, Affiliates of Service Provider, and Service Provider Personnel will Process Company Personal Data only on behalf of and for the benefit of Company, for the purposes of Processing Company Personal Data in connection with the Agreement, and to carry out its obligations pursuant to the Agreement and Company's written instructions. Company will have the exclusive authority to determine the purposes for and means of Processing Company Personal Data. Service Provider will ensure that its personnel who have access to Confidential Information or Company Personal Data are informed of the confidential nature of the Confidential Information or Company Personal Data through appropriate training on their responsibilities to access such types of information.

29. **Cross Border Data.** Service Provider will not, and will ensure that its Affiliates and Service Provider Personnel do not, Process, disseminate, or transfer Company Personal Data outside the country (or, if it was originally delivered to a location inside the European Economic Area ("**EEA**") or Switzerland, outside the EEA or Switzerland) to which Company or its respective personnel originally delivered it for Processing (a "**Cross-Border Data Transfer**") without the explicit prior written consent of Company or the appropriate Affiliate of Company, which may be withheld in its sole discretion. Service Provider shall enter into any written agreements as are necessary (in Company's reasonable determination) to comply with Data Privacy Laws concerning any cross-border transfer of Company Personal Data, whether to or from Service Provider.

30. **Information Security Incident Response.** Service Provider shall maintain security incident management policies and procedures, including detailed security incident escalation procedures. In the event of any Information Security Incident, Service Provider will, at its sole expense: (a) expeditiously (but in no case later than twenty-four (24) hours after Service Provider, an Affiliate of Service Provider, or Service Provider Personnel learns of an Information Security Incident) report such Information Security Incident to Company, summarizing in reasonable detail the effect on Company, the Company Systems, or the business reputation of Company, if known; (b) investigate (with Company's participation or the participation of an independent third party forensic investigator if requested by Company) such Information Security Incident and cooperate with Company and its designees in respect of any investigation by Company of or any such Person relating to security or Information Security Incident, including, but not limited to, providing any information or material relevant to such security breach in Service Provider's possession or control or in the possession or control of any Service Provider Personnel or any Subcontractor; (c) perform a risk assessment and develop a corrective action plan and provide a written report to Company of such risk assessment and action plan taken or to be taken by Service Provider; (d) prepare and (following Company's approval) implement a remediation plan to take all necessary and advisable corrective actions and cooperate fully with Company in all reasonable and lawful efforts to prevent, mitigate, rectify and remediate the effects of the Information Security Incident; (e) ensure that such report contains all information necessary to: (i) conduct an appropriate legal analysis to determine compliance with all applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective (including, without limitation, Data Privacy Laws); and (ii) determine the extent to which notification and communication to the Affected Persons (defined below) is advisable or required by any applicable laws; (f) make all involved Service Provider Personnel available for interview; (g) mitigate, as expeditiously as possible and to the extent practicable, any harmful effect of such Information Security Incident that is known to Service Provider, Affiliates of Service Provider or Service Provider Personnel; (h) cooperate with Company and its respective personnel in providing any filings, communications, notices, press releases or reports related to any Information Security Incident; and (i) cooperate with Company and its designees in respect of implementing new security measures to help prevent such occurrences from being repeated. The content of any filings, communications, notices, press releases or reports related to any Information Security Incident must be approved by Company prior to any publication or communication thereof.

31. **Information Security Incident Expenses.** In addition to the indemnification obligations of Service Provider set forth in the Agreement, Service Provider will defend, indemnify and hold Company, and its respective officers, directors, employees and agents, harmless from and against any and all claims, suits, causes of action, liability, loss, costs and damages, including reasonable attorney fees, arising out of or relating to any Information Security Incident including but not limited to: (a) expenses incurred to provide warning or notice to Company's former and current employees, suppliers, customers, and other Persons whose Company Personal Data may have been disclosed or compromised as a result of the Information Security Incident (the "**Affected Persons**") and to law-enforcement agencies, regulatory bodies or other third parties as required to comply with law, including Data Privacy Laws, or as otherwise directed by Company; (b) expenses incurred either by Company or through Company's retention of an independent third party forensic

investigator, legal counsel, or any other third party, to investigate, assess, or remediate the Information Security Incident and to comply with applicable laws and/or relevant industry standards; (c) 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 applicable laws or recommended by one or more of Company's regulators or any other similar protective measures designed to mitigate any damages to the Affected Persons; (d) expenses incurred to retain a call center or to develop any internal or external communication materials in order to respond to inquiries regarding the Information Security Incident for a period of at least one hundred eighty (180) days or such longer time as is required by law; (e) fines, penalties, or interest that Company pays to any governmental or Regulatory authority; (f) legal expenses incurred in connection with an Information Security Incident or to address any claims by third parties as a result of the Information Security Incident or investigation by law-enforcement agencies or regulatory bodies; (g) expenses incurred to the retention of a public relations or crisis management firm in order to manage communications on behalf of Company related to any Information Security Incident, and (h) costs of ransomware requests, recovery efforts from ransomware, and business loss from ransomware. Without limiting, precluding, or reducing Company's entitlement to damages of any type under the Agreement or Service Provider's indemnification obligations or liability to Company, the expenses stated in the foregoing (a)-(h) are considered additional direct damages of Company.

32. **No Violation of Privacy and Information Security Requirements.** Service Provider represents and warrants that no applicable law, or legal requirement, or privacy or information security enforcement action, investigation, litigation, or claim prohibits Service Provider from: (a) fulfilling its obligations under the Agreement; or (b) complying with instructions it receives from Company concerning Company Confidential Information. Service Provider further represents and warrants that neither it nor a Subcontractor or Affiliate will access or otherwise obtain Company Confidential Information or connect in any way to Company Systems unless the safeguards and security measures described in this Data Security Addendum have been fully implemented and are effective. Service Provider will enter into any further privacy or information security agreement reasonably requested by Company.

33. **Lost or Improperly Destroyed Company Confidential Information.** Service Provider will not, and will not permit any Affiliates of Service Provider or Service Provider Personnel to, delete or destroy any Company Confidential Information or media on which Company Confidential Information resides without prior authorization from Company. Company hereby authorizes Service Provider to delete or destroy Company Confidential Information in accordance with any Company document retention policies or as otherwise directed by Company in writing. Service Provider will, and will cause its Affiliates and Service Provider Personnel to, maintain and provide to Company one or more reports that identify the Company Confidential Information, including media, that has been destroyed and sanitized as applicable in accordance with the then most current version National Institute of Standards and Technology or ("**NIST**") special publication 800-88 Rev. 1 Guidelines for Media Sanitization. In the event any Company Confidential Information is lost or destroyed due to any act or omission of Service Provider, Affiliates of Service Provider, or Service Provider Personnel, including any Information Security Incident, Service Provider will restore or will cause the applicable Service Provider Affiliate or Subcontractor to restore such Company Confidential Information using the most recent available back-up. Service Provider will prioritize this effort to minimize any adverse effect upon the business of Company and use of the Services and the Service Provider Systems. Company agrees to cooperate with Service Provider to provide any available information, files, or raw data needed for the regeneration, reconstruction, or replacement of the Company Confidential Information. If Service Provider or the applicable Service Provider Affiliate or Subcontractor fails to fully regenerate, reconstruct and/or replace any lost or destroyed Company Confidential Information within the time reasonably set by Company, then Company may, at Service Provider's expense, obtain data reconstruction services from a third party, and Service Provider will cooperate, and will cause the applicable Affiliate of Service Provider, Subcontractor, or Service Provider Personnel to cooperate with such third party as requested by Company. If it is determined that Company Confidential Information has been lost or destroyed as a result of the willful, intentional, or negligent acts or omissions of Service Provider, an Affiliate of Service Provider, Subcontractor, or Service Provider Personnel, Company may terminate the Agreement for cause and pursue any civil and criminal actions available to it.

34. **Return or Intentional Destruction of Company Confidential Information.** Service Provider will, and will cause its Affiliates and Service Provider Personnel to, permanently delete and destroy Company Confidential Information (or the portion of such Company Confidential Information specified by Company) and/or will return such Company Confidential Information to Company or Company's designees, in the format and on the media prescribed by Company, as follows: (a) within thirty (30) days from the expiration or termination of the Agreement and completion of each party's obligations hereunder and; (b) at any time Company requests Company Confidential Information or within thirty (30) days from Company's request. Service Provider will deliver to Company written certification of its compliance with this paragraph and the compliance by its Affiliates and Service Provider Personnel signed by an authorized representative of Service Provider. Where it is not technically feasible and/or commercially practicable for Service Provider or a Service Provider Affiliate or Subcontractor to permanently delete or destroy Company Confidential Information held in electronic form, Service Provider will permanently delete or destroy Company Confidential Information once it becomes technically feasible and/or commercially reasonable to do so. In the interim, Service Provider will ensure, and will cause its Affiliates and Service Provider Personnel to ensure, that any residual Company Confidential Information which is retained under its custody or control is permanently put beyond use and not Processed any further save for the mere retention of such residual information. If it is not technically feasible and/or commercially practicable to permanently put Company Confidential Information beyond use and not Process such information any further, then Service Provider and its Affiliates and Service Provider Personnel will continue to apply the protections set forth hereunder for the Company Confidential Information until such Company Confidential Information is put beyond use. In no event will Service Provider, or any Service Provider Affiliate or Subcontractor withhold any Company Confidential Information as a means of resolving any dispute.

35. **Indemnity.** In addition to any other indemnification obligation contained in the Agreement, Service Provider shall indemnify, defend and hold Company, its officers, directors, employees, parent, and subsidiaries, harmless from and against any and all claims, demands, losses, liabilities, costs and expenses, including attorneys' fees and in-house counsel fees, arising from a breach of this Data Security Addendum by Service Provider, its employees, agents, representatives, or Service Provider Personnel from acts or omissions of Service Provider or Service Provider Personnel relating to Company Confidential Information.

36. **Electronic Discovery.** Service Provider shall maintain end-to-end electronic discovery capabilities consistent with generally acceptable standards and compliant with all regulations and laws. At a minimum, Service Provider shall perform the following functions: (a) upon receiving written notice from Company to preserve and collect electronic data relevant to a matter, Service Provider shall take reasonable and immediate steps to preserve and Collect all electronic data relevant to a case; (b) Service Provider shall maintain detailed documentation of all activities related to the preservation and collection of electronic data; and (c) at the request of Company's legal counsel or its designated representative, Service Provider shall search collected data and provide the results to Company or its designated third party.

37. **Data Subject Access, Correction and Portability Requests.** Service Provider will promptly notify Company in writing, and in any case within two (2) days of receipt to security@lpcorp.com, if Service Provider receives: (a) any requests from an individual with respect to Company Personal Data including, but not limited to, opt-out requests, requests for access and/or rectification, blocking, erasure, requests for data portability; or (b) any complaint, objection,

notice or other communication relating to Company Personal Data or either party's compliance with applicable law in relation to Company Personal Data including, but not limited to, allegations that the Processing infringes an individual's rights under applicable law. Service Provider will not directly respond to any such request, complaint, notice, or other communication unless expressly authorized to do so by Company or required by applicable law, and it will provide Company with reasonable cooperation and assistance in relation to any such request, complaint, notice, or communication. Additionally, Service Provider shall ensure that it has implemented technical and organizational measures to assist Company in fulfilling its obligations to respond to any such requests from an individual with respect to Company Personal Data.

38. **New Products.** Service Provider may not provide any new service or product in connection with the Services, without first obtaining either: (a) consent from Company permitting such change; or (b) a fully executed amendment to this Data Security Addendum addressing such change. Company will not be liable to Service Provider or its Affiliate and will not incur any payment obligations for products or services not accepted due to the lack of both (a) and (b). The acceptance of a new product or service without (a) or (b) above does not constitute a waiver of any rights or obligations under the Agreement and this Data Security Addendum. A breach of this Section by Service Provider is deemed a material breach of the Agreement.

39. **Modifications of Terms.** This Data Security Addendum shall not be modified except by written amendment signed by the Parties.

40. **Further Assurances.** Service Provider will take any other steps reasonably requested by Company to assist Company in complying with any notification, registration, or other obligations applicable to Company under applicable laws, rules, and regulations with respect to Company Data. Such steps may include, without limitation, executing such additional or supplemental agreements required by applicable laws and regulations.

41. **Headings; Interpretations.** The descriptive headings of the sections of this Data Security Addendum are inserted for convenience only and shall not control or affect the meaning or construction of any provision hereof. In this Data Security Addendum, unless the context otherwise requires: (a) the term "days" means calendar days; and (b) the term "including" shall mean, "including, without limitation."