Note to Vendor

This page should not be included in the contracting documents; it is to provide guidance to the vendor.

The UPS Information Security Exhibit is a standard document provided to UPS vendors for both on-premises and cloud solutions where a vendor will likely:

- Have access to or be able to access UPS Data or/and UPS Systems
- Collect and process data on behalf of UPS or while providing the service
- Provide technology or equipment-related information
- Provides technology platforms or services where UPS Data is hosted

The exhibit is designed to govern the entire relationship UPS may have with the vendors, current and potential, and all types of services that may arise with a vendor. The ISA document broadly outlines the following:

- Minimum enterprise security controls and capability expectations informing the vendor's information security program capabilities
- Minimum security controls for the specific service(s) or product(s) being negotiated, taking into account future services that may be provided
- Note that only controls in scope will apply for the purpose of each engagement. However, capabilities need to be established for potential engagements, and for terms the vendor feels will not apply, the vendor must be able to show how the terms will never apply.

UPS recognizes that there are different approaches to achieving control objectives. If the approach differs from the minimum control stated in the exhibit, the vendor should document in reasonable detail how the control objective is achieved.

UPS INFORMATION SECURITY EXHIBIT

1. GENERAL

(a) This UPS Information Security Exhibit (the "Exhibit") outlines the logical and physical security requirements that Vendor will maintain as part of the Services ("Security Requirements"). The Security Requirements are applicable to the Information Security Program(s) of the Vendor, as well as all Vendor Controlled facilities that contain UPS Data and/or access UPS Systems, and/or support UPS Information Technology (IT) services or products. Capitalized terms used in this Exhibit without a definition will have the meaning ascribed to them in the Agreement.

(b) Definitions:

(i) "Affiliate" means an entity that a party controls or is controlled by, or with which a party is under common control. For purposes of this definition, "control" means ownership of more than fifty (50%) percent of the voting stock or equivalent ownership interest in an entity.

(ii) "Agreement" as used in this Exhibit will be the document/artifact such as the Master Service Agreement (MSA), Purchase Order, or other document used to procure the goods/products/services from Vendor by UPS.

(iii) "Applicable Law" means all applicable laws (including those arising under common law), statutes, codes, rules, regulations, reporting or licensing requirements, ordinances, and other pronouncements, as interpreted or enforced by relevant governmental or regulatory authorities.

(iv) "Confidential UPS Data" means the data deemed "Confidential Information" under the Agreement and any Personal Information, including but not limited to, Sensitive Personal Information.

(v) "Personal Information" means information that identifies or relates to an identifiable individual (i.e., a person who can be identified, directly or indirectly, including, by reference to an identification number, location data, an online identifier or to one or more factors specific to the person's physical, physiological, mental, economic, cultural, or social identity) and such similar data regulated under Applicable Law.

(vi) "Privileged Users" means any users who have enhanced authority to access and configure networked systems, including but not limited to system administrators and "super users" who can provision, install, upgrade, or modify credentials, operating systems, source code, applications, and other networked systems.

(vii) "Secured" means physical and logical, as applicable, methods of security designed to protect against unauthorized access, acquisition, modification, theft, misuse, or destruction of information. These methods may incorporate recommendations in specific publications of the National Institute of Standards and Technology ("NIST"), the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC"), Federal Information Processing Standards ("FIPS"), or the Internet Engineering Task Force ("IETF") and specific protocols such as Transport Layer Security ("TLS"), or the Advanced Encryption Standard ("AES").

(viii) "Sensitive Personal Information" means a financial account number, such as a bank account number, credit card number or debit card number, a Social Security Number or other national insurance number, a driver's license number or other government identification number, a date of birth, an email address or username in combination with a password or security code for an online account, a private key or digital signature, biometric data of a specific person, precise geolocation data, or credit history or eligibility information that is identifiable to a specific person; or information that reveals racial or ethnic origin, political opinions, religious or spiritual beliefs, criminal history, or labor union membership of an identifiable person or that relates to a specific person's health or sex life and such similar information regulated under Applicable Law.

(ix) "Services" as used in this Exhibit shall mean the services, goods, or work provided by the Vendor in the Agreement and has the same meaning as the term "Work," "Services," "Goods," or "Deliverables" if used in the Agreement.

(x) "UPS" as used in this Exhibit means the UPS entity to the Agreement and has the same meaning as the term "Owner," "UPS," or "Purchaser" if used in the Agreement.

(xi) "UPS Data" means any data transmitted by UPS or its Affiliates to Vendor or accessed or acquired by Vendor in connection with the provision of Services.

(xii) "UPS Systems" means, collectively, the systems of UPS and its Affiliates, managed by UPS and accessed or hosted by Vendor in connection with the provision of Services, including computer systems, software, and networks, including technology and data, stored on or accessible through utilization of such systems, software, and networks.

(xiii) "Vendor" as used in this Exhibit means the counterparty to UPS in the Agreement or has the same meaning as the term "Supplier," "Seller," "Provider," "Contractor," or "Consultant" if used in the Agreement.

(xiv) "Vendor Personnel" means the Affiliates, officers, directors, employees, agents, contractors, consultants, vendors, invitees, and representatives of Vendor and of Vendor's Affiliates.

(c) Vendor will (i) implement and maintain a comprehensive written information security program; (ii) update and/or review such program, as necessary, on no less than an annual basis or upon a material change in the provision of Services; and (iii) ensure such program

(1) complies with Applicable Law and applicable industry standards, examples of relevant industry standards that may be applicable include:

- ISO/IEC 27001:2022
- ISO/27002:2013/2022
- ISO27017
- ISO27018
- Payment Card Industry Data Security Standard (PCI DSS)
- US NIST Cybersecurity Framework
- US NIST 800-53
- US NIST800-171
- Committee of Sponsoring Organizations (COSO)

(2) includes appropriate administrative, logical, technical, and physical safeguards that align with this Exhibit and

(3) is designed to achieve the following objectives:

(A) To ensure the security and the confidentiality, integrity, and availability of UPS Data

(B) To protect against any threats or hazards to the security and integrity or availability of UPS Systems

(C) To prevent unauthorized or accidental access, acquisition, destruction, loss, deletion, disclosure, or alteration or use of UPS Data or UPS Systems

(d) Any expenses related to the implementation and maintenance of the Vendor's Information Security program, and the requirements and obligations set forth in this Exhibit, are the sole responsibility of the Vendor.

(e) Where Applicable Law prevents compliance with the Security Requirements, Vendor is responsible for notifying UPS in order to determine appropriate compensating controls. Where Applicable Law sets forth more stringent requirements than those set forth in this Exhibit, Vendor will comply with Applicable Law.

(f) The provisions of this Exhibit will control in the event of a conflict between the Agreement (including any attachments, exhibits or schedules) and this Exhibit.

(g) Vendor will disclose to UPS any shared third-party hosting facilities that will hold UPS Data, and Vendor will take reasonable measures to ensure such third parties materially comply with the applicable terms of this Exhibit.

(h) For the avoidance of doubt, and in addition to the confidentiality obligations contained in the Agreement, when making any authorized transfer of UPS Data hereunder, Vendor will comply with Applicable Law and this Exhibit.

(i) If the underlying Agreement involves Personal Information, Vendor will execute the UPS Data Processing Exhibit (DPE). The Data Transfer Addendum (DTA) and Transfer Impact Assessment (TIA) are also needed where personal data is transferred out of or accessed from outside of the European Economic Area (EEA) or the UK. Vendor will execute any additional privacy documentation where required by Applicable Laws.

(j) If the underlying Agreement involves artificial intelligence, large language model or machine learning technology, Vendor will execute the UPS Artificial Intelligence Addendum.

2. POLICIES, AWARENESS AND TRAINING

(a) Vendor will maintain, publish, recertify, enforce, and make available to UPS upon request, written policies addressing core information security concepts including, but not limited to, "acceptable use," "physical asset management," "encryption," "password management," "security incident and data breach response," "artificial intelligence" "physical security," "disaster recovery," and "background checks."

(b) Vendor will provide training on a general range of information security topics, including, but not limited to phishing and social engineering, strong passwords, and removable media to all existing Vendor Personnel on an annual basis, and to new Vendor Personnel upon hire, to educate such Vendor Personnel about information security industry standards and best practices, and emerging threats and trends. Vendor will provide copies of training materials to UPS upon request.

3. ASSET MANAGEMENT

(a) Vendor will establish and maintain an asset management program which includes asset inventory (cataloging and tracking), recording of baseline configurations, asset ownership, asset location, asset classification, asset decommissioning and disposal.

(b) Vendor will maintain sufficient technology and capability to apply information classification schemes and storage requirements across the organization (on-premises and in the cloud) according to legal or regulatory requirements, business value, and sensitivity to unauthorized disclosure or modification.

(c) Vendor will maintain an automated asset inventory discovery tool to inventory assets on the network, identify new devices, document IP addresses and operating system and software versions on the network. The asset inventory must be maintained and periodically reviewed in line with defined schedules and standards.

(d) Vendor will implement replacement or mitigation strategies for end of life and legacy infrastructure, networks, operating systems, and software applications.

4. ACCESS MANAGEMENT AND IDENTIFICATION; AUTHENTICATION

(a) Vendor will permit only those Vendor Personnel and third parties who are authorized pursuant to the Agreement to access UPS Data or UPS Systems. Authorized Vendor Personnel and authorized third parties will use UPS Data or UPS Systems only as necessary to perform their obligations under the Agreement and this Exhibit.

(b) Vendor will follow Applicable Law and applicable industry standards to authenticate and authorize users. Vendor will not use shared or generic identification credentials to access UPS Data or UPS Systems. Passwords must contain a minimum of twelve (12) characters and include at least one alpha character, one symbol, and one numeric character. In addition, user IDs must be deactivated after no more than ten (10) failed log-in attempts.

(c) When applicable, Vendor will identify to UPS any Vendor Personnel requiring access to UPS Systems. Vendor Personnel are required to use multi-factor authentication technology to access UPS Systems. UPS will issue multi-factor authentication technology to Vendor Personnel. Vendor will promptly notify UPS when Vendor Personnel no longer requires access to UPS Systems.

(d) Vendor will maintain a documented centralized repository of all identification credentials used to access Vendor's network and /or systems where UPS Data or UPS Systems reside. Vendor will immediately revoke access from Vendor Personnel and authorized third parties who no longer require access to UPS Data or Systems.

(e) Vendor will periodically review and revoke access rights of users, as needed, and will log, monitor, and provide to UPS, upon request, reports on identification credentials used to access UPS Data or UPS Systems.

(f) Authentication to Vendor's network resources, platforms, devices, servers, workstations, applications, and devices must not be allowed with default passwords and must use role-based access control, and either single sign-on (SSO), federated identity management (FIM) or similar principle. Multi-factor authentication must be used for (i) Vendor's Users, (ii) remote access to Vendor's network, (iii) regulated environment and (iv) access to Confidential UPS Data.

(g) Vendor's application(s)/supplied product(s) shall provide a single sign-on (SSO) mechanism that supports the OpenID Connect (OIDC) with Proof Key for Code Exchange (PKCE), Security Assertion Markup Language (SAML) v2.0 or greater, or Open Authorization (OAuth) 2.0. Additionally, application(s)/supplied product(s) will support integration with external identity providers (e.g., Microsoft Entra Active Directory) and support multi-factor and/or two (2) factor authentication. In cases where an application(s)/supplied product(s) needs to access a Microsoft Entra ID resource programmatically, a Service Principal (SP) must be used implementing the client credential flow with certificate-based authentication, not a client secret.

(h) All access to UPS Data and UPS Systems, if applicable, will be via a Secured connection between Vendor's service locations (including access through any of Vendor's cloud service providers) and UPS.

(i) Vendor will ensure secure external network connections to Vendor's network occur via secure connections (e.g., Virtual Private Network (VPN) or similar technologies).

5. PRIVILEGED ACCESS

Vendor will assert that Vendor's security program adheres to the following principles:

(a) Maintaining an inventory of all privileged accounts including domain(s) and local accounts to ensure only authorized and approved individuals have privileged access to systems and resources.

(b) Provide specific Privileged User role training to persons with privileged access.

(c) Ensure privileged access is only granted on least privileged basis and without violating the separation of duties principle.

(d) Performance of periodic (quarterly) reviews and recertification of privileged access to ensure privileges are appropriately assigned to users based on their job responsibilities.

(e) Defining and implementing a privileged access request process to ensure privileged access roles and rights are granted for a time limited period and implement procedures to prevent the culmination of segregated privileged access.

(f) Implementing Multi-Factor Authentication (MFA) and encrypted login channels for all privileged account access.

(g) Use of dedicated or secondary account/systems for elevated, privileged functions.

(h) Configuration of the privilege account systems to log and alert on key changes such as added or removed accounts, unsuccessful logins, or similar activities.

6. SECURE DATA HANDLING

(a) Vendor will encrypt Confidential UPS Data at rest, in transit, and in use via AES minimum 256-bit encryption and 2048-bit cipher key length.

(b) Vendor will apply and maintain full disk encryption to any UPS Data at rest on Vendor's systems that access, transmit, or store UPS Data.

(c) Any encryption products used by Vendor must be FIPS 140-2 or 140-3 certified, or at least meet FIPS 140-2 or 140-3 applicable standards. Vendor must use TLS or equivalent with the highest feasible encryption available when transferring UPS Data over the Internet.

(d) Symmetric encryption keys and asymmetric private keys will be encrypted in transit and storage, protected from unauthorized access, and Secured. Cryptographic key management and rotation procedures must be documented. Access to encryption keys must be restricted to named administrators. Vendor will follow industry standards, such as NIST 800-57 or ISO recommendations, to generate, store, and manage cryptographic keys used to encrypt UPS Data.

(e) Vendor will maintain secure data disposal procedures, including but not limited to using secure erase commands, degaussing, and "crypto shredding" when needed. Vendor's procedures will follow industry standards, such as NIST 800-88 or ISO recommendations.

(f) Vendor must have a capability and process at the end of the contracted term to securely return and securely delete or destroy UPS Data from Vendor's environment. Upon UPS request, Vendor will provide evidence or authorized attestation of such deletion or destruction.

(g) Vendor will have the capability to perform a remote wipe on any Vendor Personnel mobile device, including, but not limited to a smartphone, tablet, and laptop ("Mobile Device"). If any Mobile Device contains or has access to UPS Data, Vendor will have a capability to wipe the Mobile Device upon a remote command after (i) multiple failed attempts to authenticate the user of the Mobile Device or (ii) the Mobile Device has been lost or stolen.

(h) Vendor will deploy Data Loss Prevention (DLP) technology, processes, and/or solutions to protect and prevent against exfiltration of UPS Data or transfer of UPS data to non-authorized assets or networks.

7. PHYSICAL AND ENVIRONMENTAL SECURITY

(a) Vendor's facilities, if any, must maintain appropriate physical and environmental controls such as access restriction, detective monitoring controls, fire detection and suppression, climate control and monitoring, power and backup power solutions, and water damage detection.

(b) Vendor will implement appropriate physical access controls such as user authentication badge access and/or appropriate sign-in procedures and appropriate access logs for facilities that contain systems with access to UPS Systems and UPS Data.

8. ENDPOINT & NETWORK SECURITY

(a) Vendor will install, configure, and maintain perimeter and network security controls to prevent unauthorized access to UPS Data and UPS Systems and/or Vendor's network and systems. Examples of security controls include, but are not limited to, firewalls, switches, routers, wireless access points, intrusion detection systems ("IDS"), intrusion prevention systems ("IPS"), anti-malware software, and access control lists.

(b) Vendor will maintain and configure endpoint security software on servers, desktops, laptops, mobile, and portable digital media devices, including but not limited to updated anti-virus software. Other endpoint protections may include encryption software, intrusion detection systems, intrusion prevention systems, anti-malware software, in accordance with industry standards. Vendor will ensure such configurations generate alerts to Vendor, logs are accessible by Vendor, and Vendor will provide to UPS upon request.

(c) Vendor will have a security operations center ("SOC"), or a team performing a similar function, responsible for, at a minimum, security information and event management ("SIEM"), security logging, continuous security monitoring, and secure network security configurations.

(d) Vendor's Infrastructure and network components shall be designed, developed, deployed, and configured such that UPS Data and user access are appropriately segmented and restricted from other tenants or users. UPS Data will be logically, separated from that of other customers via data segmentation and containerization.

(e) Vendor will implement and maintain security and hardening standards for network devices, including, but not limited to, baseline configurations, patching, passwords, access control, and multi-factor authentication with automatic system logout after ten (10) minutes but no more than twenty (20) minutes of inactivity.

(f) Vendor will use defense-in-depth techniques, including, but not limited to, deep packet analysis, traffic throttling, and packet black-holing, for the detection of and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.

(g) Vendor will follow documented change management procedures.

(h) Vendor will reasonably protect workstations from intrusion by implementing automatic screen savers, locking devices, privacy screens, and/or similar controls.

9. APPLICATION SECURITY

(a) Vendor will follow secure software development life cycle ("SDLC") secure coding practices, in accordance with the most current guidance per the following (i) the Open Web Application Security Project ("OWASP") (found at https://owasp.org/Top10/), (ii) Common Weakness Enumeration ("CWE") (found at "https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html) and (iii) SANS guidance Most Dangerous Software Errors (found at https://www.sans.org/top25-software-errors/), to ensure harmful code is not delivered and best practices are followed. Coding practices will include (i) regular security code reviews; and (ii) static and dynamic scanning of all software and/or applications storing, processing, and/or transmitting UPS Data.

(b) Vendor will maintain proper segmentation of data environments (Development, Test, and Production). Segregation/Segmentation must be employed such that production data will not be used in development and testing environments.

(c) Vendor will develop systems, products, and business practices based upon a principle of privacy by design and industry standards. Vendor will ensure that systems' privacy settings are configured according to all applicable laws and regulations.

10. RISK MANAGEMENT; THIRD PARTY/VENDOR ASSURANCE

(a) Vendor will maintain a third-party risk management program. This will include (i) maintenance of information security agreements to ensure that Vendor's third parties are bound to the terms of this Exhibit; and (ii) monitoring and auditing (at least annually) of Vendor's third parties. Vendor will make available to UPS upon request, audit and monitoring reports, information security agreements, and other artifacts of Vendor's third parties.

(b) Risk management will include remediation by Vendor of any identified findings commensurate with risk and evidence of completion.

(c) Vendor will maintain a risk assessment program, which will define roles and responsibilities for performing risk assessment and responding to results. Vendor will perform an annual risk assessment to verify the design of controls that protect business operations and information technology.

(d) Vendor will maintain a risk assessment remediation plan, which will include the use of issue tracking to completion that measures remediation progress regularly against target dates. Vendor will assign an owner (active Vendor Personnel) to each remediation plan. For risk acceptance, Vendor management will provide clear acknowledgement and a description of the risk. The risk acceptance must include a business justification.

11. VULNERABILITY AND PATCH MANAGEMENT

(a) Vendor will cooperate with UPS to conduct security vulnerability scans of Vendor's systems and networks that access or store UPS Data. Such security vulnerability scans shall be based on the requirements set forth in UPS Application Security Checklist ("Security Checklist"). In the event that UPS identifies vulnerabilities, Vendor agrees to promptly remediate identified vulnerabilities in line with the agreed patching cadence.

(b) Vendor will perform routine network and application-level scans for vulnerabilities, intrusions, and unauthorized changes to UPS Data or UPS Systems (each a "Vulnerability Scan") at least quarterly and prior to network and application provisioning.

(c) At least once every year, or upon request from UPS following a Vendor related Security Breach, Vendor will hire an independent third-party cybersecurity firm to test a potential unauthorized user's ability to penetrate Vendor's network (a "Penetration Test").

(d) At UPS's request, Vendor will provide the reports generated by Vendor's Vulnerability Scans and Penetration Tests, and promptly correct all identified vulnerabilities in accordance with the agreed patching cadence.

(e) Vendor will identify, triage, document, and remediate vulnerabilities and threats to UPS Data and UPS Systems, including those identified by anti-virus scans, firewall reports, IPS or IDS alerts, vulnerability scans, penetration tests, or other security data. Vendor will determine the severity of each vulnerability or threat in accordance with the NIST National Vulnerability Database's ("NVD") Common Vulnerability Scoring System ("CVSS"), version 3.0 or higher (found at https://nvd.nist.gov). Vendor will notify UPS promptly, but no more than 72 hours, after discovery of identified "high" and "critical" vulnerabilities or threats to UPS Data or UPS Systems, as determined by the CVSS formula.

(f) Vendor will apply security patches and system updates to Vendor's network, systems, software, applications, appliances, and operating systems in the Vendor's environment in a reasonable time frame based on the criticality of an identified vulnerability, availability of the patch, and sensitivity of the underlying data, but at a minimum, Vendor will test and apply patches upon their availability based on the following schedule from the general release date: (i) Critical: within 3-5 days; (ii) High: within 10 days; and (iii) Other: within 30 days.

(g) Where the Vendor solely supplies UPS with commercial software or cloud software or hardware services, Vendor will supply, deliver, or apply security patches and system updates to vendor-managed and/or supplied software and applications, appliances, devices, and operating systems. The updates and patches will be supplied or applied upon the general release date based on the criticality of the vulnerability, availability of the patch, and sensitivity of the underlying data: (i) Critical: within 3-5 days; (ii) High: within 10 days; (iii) Moderate: within 20 days; (iv) Others: within 30 days. Severity will be determined in accordance with the National Vulnerability Database's Common Vulnerability Scoring System formula (found at https://www.nist.gov) and documented by Vendor.

12. BUSINESS CONTINUITY, RESILIENCE and DISASTER RECOVERY

(a) Vendor will maintain a documented and operational Business Continuity and Disaster Recovery (BC&DR) Program. Vendor will exercise and update its BC&DR plans at least annually.

(b) Vendor will document and upon request, provide to UPS copies of all contingency and incidence planning procedures relevant to the goods, software or services used by UPS in connection with this agreement, or used by the vendor to produce or support the said goods, software, or services.

(c) Vendor will cooperate with UPS in performing joint tabletop exercises of Vendor BC&DR plans, upon request by UPS.

(d) Vendor will conduct business impact analysis on critical assets to determine the acceptable Recovery Time Objective (RTO) /Recovery Point Objective (RPO) of the assets relevant to the goods, software or services provided to UPS and which may impact UPS.

(e) Vendor will periodically backup data per UPS business requirement and ensure that controls are in place to support the confidentiality, integrity, and availability of the backups, snapshot images and other recovery media.

(f) Prior to being backed up, all UPS Data will be encrypted or equivalently Secured.

(g) Vendor will monitor and test system backups to ensure the integrity of the backup for successful data restoration according to the Vendor's backup schedule and should be at minimum yearly.

(h) Vendor will verify data restoration and integrity from backups, snapshot images and other recovery media at a minimum yearly.

13. SECURITY BREACH

(a) Vendor will maintain and annually update a documented data breach action and response plan.

(b) If Vendor discovers or is notified of a breach of security, which results in unauthorized access, acquisition, disclosure, or use relating to any UPS Data or UPS Systems or any violation of these Security Requirements ("Security Breach"), Vendor will promptly at its expense: (i) notify UPS via UPS email addresses soc@ups.com and globalprivacy@ups.com of the Data Breach without undue delay, but no later than 72 hours of becoming aware of the Data Breach; (ii) investigate the Data Breach; (iii) mitigate the effects of the Data Breach; and (iv) perform post-incident assessments, including those reasonably requested by UPS, and report on the results of such assessment(s) to UPS.

(c) For any Data Breach caused by Vendor or any of its subcontractors, Vendor will be solely responsible for the costs of responding to the Data Breach, including, but not limited to, the costs to: (i) hire external counsel or litigate related claims; (ii) hire technical experts; and (iii) provide any notices and credit services to third parties, and all associated support to such third parties (e.g., call center support) and any services to third parties as required by Applicable Law.

(d) Vendor must maintain Cyber Insurance coverage at its sole cost, for technology/professional liability insurance policy including coverage for network security risk and cyber liability coverage (including coverage for unauthorized access, failure of security, breach of privacy perils, as well as notification costs and regulatory defense). Such insurance shall be in force at all times during the term of the Agreement and for a period of two years thereafter for services completed during the term of the Agreement at the appropriate amounts for business need.

14. **REPORTING AND RIGHT TO AUDIT**

(a) Vendor will perform continuous monitoring, logging, review, and mitigation of attempted and successful access by unauthorized parties. Further, Vendor will maintain security event logs for vulnerabilities, intrusions, and unauthorized changes on endpoints, network devices, and server systems that contain UPS Data or UPS Systems. All logs must be protected from unauthorized access or modification and be configured so as not to capture and record Confidential UPS Data and shall be provided to UPS upon request.

(b) Vendor will cooperate with UPS in any investigations of possible fraudulent or unauthorized use of or access to UPS Data or UPS Systems by Vendor's employees or third parties. If deemed necessary by UPS, Vendor will cooperate with UPS in conducting security vulnerability scans of Vendor's systems and networks that access or store UPS Data.

(c) UPS reserves the right to perform cybersecurity audits/assessments, with Vendor's cooperation, at least annually and may reasonably request additional assessments following a Security Breach. The audit may be on-site at Vendor's facility, via questionnaire, or through a third party. UPS will provide Vendor with 30 days' notice prior to the audit. Vendor will respond to all questionnaires and resulting recommendations within 30 days or as otherwise agreed by the parties.

(d) Vendor agrees to discuss any findings with UPS, and to provide related evidence of capabilities, remediation, and compliance activities.

(e) Vendor agrees to cooperate with UPS, as needed, to respond to internal security risk assessment questions and requests for evidence of controls in the application or systems that host or process.

By executing this Exhibit, Vendor warrants that it understands the restrictions on Vendor's use, processing, disclosure, and retention of any UPS Data. UPS from time to time, may update this Exhibit at its sole discretion and Vendor and UPS must execute the most current UPS Exhibit as requested by UPS.