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 minimum logical and physical security requirements that Vendor is required to implement and maintain as part of the Services ("Security Requirements"). The Security Requirements are applicable to the Information Security Program(s) of the Vendor, all Vendor managed environments, and any facilities or systems that store, process, or transmit 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.th

(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, at least annually or upon a material change in the provision of Services; and (iii) ensure that such program:

(1) is in accordance with Applicable Law and the current available revisions of industry standard frameworks NIST SP 800-53, and ISO.

(2) includes appropriate administrative, logical, technical, and physical safeguards consistent with this Exhibit and is designed to ensure the security, confidentiality, integrity, and availability of UPS Data and UPS Systems; protect against threats; and prevent unauthorized and accidental access, acquisition, destruction, loss, deletion, disclosure, alteration, or use of UPS Data or UPS Systems.

(d) Any costs and expenses related to the implementation, maintenance, and compliance of the Vendor's Information Security program, including 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 imposes more stringent requirements than those set forth in this Exhibit, Vendor will comply with Applicable Law.

(f) The provisions of this Exhibit shall prevail with respect to information security obligations in the event of a conflict between the Agreement (including any attachments, exhibits or schedules) and the terms of 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) Where the Agreement involves the processing of 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) Where the Agreement involves the use of artificial intelligence, large language model, machine learning, or similar technologies, 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. These policies shall be reviewed and recertified at least annually and must reflect current industry standards and regulatory requirements.

(b) Vendor will provide training to all Vendor Personnel on a general range of information security topics. Training will be conducted at least annually for existing Vendor Personnel and to new Vendor Personnel upon hire.

3. ASSET MANAGEMENT

(a) Vendor will establish and maintain an asset management program which encompasses asset life cycle.

(b) The asset management program and asset inventory must be reviewed at least annually.

(c) Vendor will maintain technology and capability to enforce information classification, storage, and data protection requirements across the organization (on-premises and cloud) according to legal, regulatory requirements, business value, and sensitivity to unauthorized disclosure or modification.

(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 only permit authorized Vendor Personnel and third parties to access UPS Data or UPS Systems strictly to meet their obligations under the Agreement.

(b) Vendor will follow Applicable Law and the current available revisions of industry standards NIST SP 800-53, and ISO, for user, system, application, and service account authentication and authorization by avoiding the use of default, shared, or generic credentials and enforcing strong passwords.

(c) For UPS provisioned access to UPS Systems and/or Data, Vendor will identify any Vendor Personnel requiring access for proper provisioning. Vendor will promptly notify UPS when Vendor Personnel no longer require access to UPS Systems.

(d) For Vendor provided access to their network and/or systems, Vendor will maintain a documented centralized repository of all identification credentials. Vendor will periodically review and immediately revoke access when no longer required.

(e) Authentication to Vendor's network resources should use role-based access control and incorporate controls including single sign-on (SSO), federated identity management, or equivalent, and mandatory multi-factor authentication.

(f) Vendor's applications/supplied products shall support single sign-on (SSO) mechanism. Additionally, applications/supplied products will integrate with external identity providers (e.g., Microsoft Entra Active Directory) and support multi-factor and/or two (2) factor authentication. If applications/supplied products need to access a Microsoft Entra ID resource programmatically, a Service Principal (SP) must be used with certificate-based authentication and not a client secret.

(g) Vendor will ensure external network connections occur via secure technology such as Virtual Private Network (VPN) or equivalent connection protocols.

5. PRIVILEGED ACCESS

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

(a) Maintain an inventory of all privileged accounts (including domain and local accounts) to ensure only authorized and approved individuals have privileged access to systems and resources based on the principles of least privilege and separation of duties.

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

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

(d) Define and implement 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.

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

(f) Use of dedicated or secondary account/system for elevated, privileged functions.

(g) Configure 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 in accordance with the current available revisions of NIST SP 800-57 and ISO, and follow the general guidelines for non-deprecated crypto protocols.

(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 in accordance with the current available revisions of NIST SP 800-111 and ISO, and follow the general guidelines for non-deprecated crypto protocols.

(c) Any hardware, software, firmware encryption and key management products used by Vendor must adhere to the current available revisions of NIST SP 800-57 and ISO, and follow the general guidelines for non-deprecated crypto protocols.

(d) Symmetric encryption keys and asymmetric private keys must be encrypted in transit and at rest, 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 must adhere to the current available revisions of NIST SP 800-57 and ISO, and follow the general guidelines for non-deprecated crypto protocols, to securely generate, store, and manage cryptographic keys used to encrypt UPS Data.

(e) Vendor will maintain secure data disposal procedures for data destruction that adhere to the current available revisions of NIST SP 800-88 and ISO recommendations.

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

(g) Vendor will have a Mobile Device Management tool with the technical capability to remote wipe any Vendor Personnel mobile device, including, but not limited to smartphones, tablets, and laptops.

(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 facilities must maintain appropriate environmental controls to protect against environmental hazards, and ensure operational continuity.

(b) Vendor facilities must implement physical access controls to prevent unauthorized physical access, support incident response, and deter theft.

8. ENDPOINT & NETWORK SECURITY

(a) Vendor will install, configure, and maintain perimeter and network security controls to prevent unauthorized access to UPS Data, UPS Systems, and Vendor's network and systems.

(b) Vendor will maintain and configure endpoint security software on all assets in accordance with industry standards. Vendor will ensure such configurations generate alerts and retain accessible logs.

(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 must ensure UPS Data and user access are properly segmented and restricted, with logical separation from other tenants and customers.

(e) Vendor will implement and maintain baseline security and hardening standards for network devices in accordance with industry standards.

(f) Vendor will implement defense-in-depth techniques to provide layered and redundant security controls, enhance resilience, and protect against cybersecurity threats.

(g) Vendor will follow documented change management procedures.

(h) Vendor will implement and maintain physical and technical controls to protect workstations from intrusion.

9. APPLICATION SECURITY

(a) Vendor will follow secure software development life cycle ("SDLC") secure coding practices, which adhere to the current available revisions of NIST SP 800-53, NIST SP 800-218, and ISO to ensure the confidentiality, integrity, and availability of software systems, minimize vulnerabilities, and maintain compliance with applicable security standards and regulations.

(b) Vendor will maintain proper segmentation of data environments including development, test, and production. Segregation/Segmentation must be employed to ensure that production data will not be used in development and testing environments.

(c) Vendor will develop systems, products, and business practices based on the principle of privacy by design which adhere to the current available revisions of NIST SP 800-53 and ISO. Vendor will ensure that systems' privacy settings and configurations are compliant with Applicable Law and regulations.

10. RISK MANAGEMENTAND 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.

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

(c) Vendor will maintain an internal risk assessment program, which will define roles and responsibilities for performing risk assessments and responding to results. Vendor shall conduct periodic risk assessments to validate control design and confirm that security measures meet business and IT requirements.

(d) Vendor will maintain a risk assessment remediation process to track identified risks to completion in accordance with industry standards.

11. VULNERABILITY AND PATCH MANAGEMENT

(a) Vendor will permit UPS to conduct quarterly security vulnerability scans of Vendor's customer-facing applications that access or store UPS Data or scan a mirrored version of the production environment. Such security vulnerability scans shall be based on the requirements set forth in the UPS Application Security Checklist. In the event that UPS identifies vulnerabilities, Vendor agrees to promptly remediate identified vulnerabilities in line with the UPS Application Security Checklist requirements and as indicated in the patching cadence in (g) below.

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

(c) At least yearly, and upon request from UPS following a Vendor related Security Breach, Vendor will hire an independent third-party cybersecurity firm to conduct 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 in accordance with industry best practices. Vendor will determine the severity of each vulnerability or threat in accordance with the latest version of the NIST National Vulnerability Database's ("NVD") Common Vulnerability Scoring System ("CVSS"). If the Vendor identifies a Critical or High vulnerability with no immediately available remediation that may impact UPS Data and UPS Systems, the Vendor must notify UPS in writing within seventy-two (72) hours of such identification.

(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 the 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 supplies UPS with software or hardware services, Vendor will supply, deliver, and/or apply any security patches and system updates. 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 latest version of the National Vulnerability Database's Common Vulnerability Scoring System formula 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 and services used by UPS in connection with this agreement, or used by the Vendor to produce or support the said goods, software, and 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) and Recovery Point Objective (RPO) of the assets relevant to the goods, software and services provided to UPS that may impact UPS.

(e) Vendor will periodically backup data 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 at least annually to ensure the integrity of the backup for successful data restoration according to the Vendor's backup schedule.

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

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) In the event of a 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 two years thereafter for services completed during the term of the Agreement at the appropriate amounts for business need.

14. **THIRD PARTY ASSESSMENT**

(a) Vendor will perform continuous monitoring, logging, review, and mitigation of security threats. Vendor will maintain security event logs for relevant activities and ensure all logs are protected against unauthorized access or modification, configured to avoid capturing confidential client data, and made available to UPS upon written request.

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

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

(d) Vendor agrees to cooperate with UPS, upon request, to respond to internal security risk assessment questions and provide evidence of controls implemented in any applications or environments that host or process UPS Data or interface with UPS Systems.

By executing this Exhibit, Vendor warrants that it understands the restrictions on Vendor's use, processing, disclosure, and retention of any UPS Data. UPS may periodically update this Exhibit, at its sole discretion, and Vendor and UPS shall renegotiate and execute the most current Exhibit as mutually agreed upon by both parties.