Vertex Customer Agreement

Security Exhibit

1. **Overview.** This Security Exhibit is incorporated in the Vertex Customer Agreement, Vertex Master Agreement, or other agreement governing Customer's use of Vertex Products and Services (the "**Agreement**"). Any capitalized term used but not defined in this Exhibit has the meaning given in the Agreement. If there is a conflict or inconsistency between this Security Exhibit and any other part of the Agreement, the term that affords greater protection for Customer Data will control.

   This Security Exhibit outlines the minimum technical, organizational, and physical controls that Vertex will maintain to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

   Vertex may update this Exhibit and the specific controls and the policies that govern them to meet evolving threats and adapt to developing security technology and industry standards. These updates may occur during the term of an Order and without notice to Customer unless the update materially impacts Customer's use of Vertex Products or Services. Current and archived versions of this Exhibit will be published on the Vertex website and will be provided on request. However, no update to this Exhibit will change Customer's Order until it is renewed. If Customer's Order is renewed, the Agreement is amended to include the then-current published version of this Exhibit.

   As used in this Exhibit, the following terms have the following meanings: "**Cloud-based Service**" means a software application made available by Vertex via the internet for online access, that is specified in an Order as being delivered via On Demand or Cloud; "**Cloud Provider**" means a third-party provider of data center services used by Vertex to provide Cloud-based Services; "**Customer Data**" means data transferred by or on behalf of Customer or its Affiliates for processing or storage to a Vertex repository in connection with any Product or Service and any derivatives based on or modifications to such data, including output derived from Customer Data that Customer or Affiliates generate using the Product or Service; "**Vertex Network**" means Vertex's corporate network; and "**Vertex Personnel**" means Vertex's employees (full-time, part-time, and temporary) and subcontractors, excluding Cloud Providers.

2. **Information Security Management Program.** Vertex will implement and maintain an information security management program ("**ISMP**"). The ISMP will establish information security as a cross-organizational function, leveraging Vertex's team organization and reporting framework to identify, assess, mitigate, and report key risks. The ISMP will be owned by a cross-organizational team that will meet and confer at least quarterly to review and analyze cybersecurity trends, threats, risks, vulnerabilities, and incidents. Under the ISMP, qualified and credentialed information security professionals will own core security management functions. Vertex technical, business, and executive managers will be accountable to enforce compliance with policies and procedures governed by the ISMP.

3. **Human Resource Security.** Vertex will require Vertex Personnel to undergo background verification and screening (listed in the Screening Attachment to this Exhibit) during on-boarding to the extent permitted by law. Role-based data stewardship responsibilities for key security and information technology administrative resources will be defined, assigned, and documented. Vertex Personnel will sign nondisclosure or confidentiality agreements that obligate them to protect Vertex confidential information and Customer Data. Vertex will enforce security protocols that include timely revocation of access to systems and data and return of information assets following change in employment or termination, as applicable. Vertex Personnel will be required to complete information security awareness training during on-boarding and annually as part of Vertex's regular compliance and awareness training program. This training program will require Vertex Personnel to acknowledge and affirm their understanding of Vertex's information security and acceptable use policies, applicable reporting frameworks, and formal disciplinary mechanisms for noncompliance.

4. **Network and Services Security.** Vertex will implement and maintain information security controls to protect the Vertex Network and Customer Data that is received, processed, or stored by Vertex and Cloud Providers in connection with Customer's use of Cloud-based Services. These controls will be designed to ensure the confidentiality, integrity, and availability of Customer Data, the Vertex Network, and information technology assets used by Vertex. They will include technical and organizational measures and other safeguards to (a) secure Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access; (b) identify and mitigate reasonably foreseeable external and internal risks to the Vertex Network and Cloud-based Services, including risks of unauthorized access to facilities, systems, and information assets storing or processing Customer Data; and (c) enable Vertex and Customer to comply with their respective obligations under applicable data privacy and data protection laws and regulations (collectively, "**Data Protection Laws**"), including the General Data Protection Regulation (EU 2016/679) and California Consumer Privacy Act. Vertex's security controls will align with applicable industry standards for cybersecurity risk management, including the NIST Cybersecurity Framework. All controls will be governed by written policies and procedures under Vertex's ISMP. All policies and procedures will be reviewed and approved annually by appropriate management-level Vertex Personnel.

5. **Specific Technical Controls.** Vertex will employ defenses such as encryption, intrusion prevention and detection, log monitoring, threat monitoring, endpoint protection, and firewalls to protect the Vertex Network, Cloud-based Services, and Customer Data, including the following, consistent with industry standards:

   5.1 full disk encryption and content filtering on laptops issued to Vertex Personnel, with external connection to the Vertex Network restricted to encrypted VPN via multi-factor authentication;

   5.2 encryption of Customer Data processed and stored in Cloud-based Services (including Customer user passwords), leveraging at least AES 256-bit encryption for data at rest (production and backup) and Transport Layer Security (TLS) 1.2 or higher for data in transit over untrusted networks;

   5.3 least privilege access to Cloud Provider environments by Vertex Personnel (reviewed quarterly), with all access via the Vertex Network;

   5.4 network-based vulnerability scanning for Vertex Network and Cloud-based Services, with regular application of patches and security updates to Vertex-issued laptops, the Vertex Network, Cloud-based Services, and associated information assets;

   5.5 intrusion prevention and intrusion detection systems (IPS/IDS), with secure storage and regular monitoring of logs;

   5.6 firewalls to control traffic to and from the Vertex Network and Cloud-based Services, with network perimeter monitoring, automated notification of suspicious activity, and rule set validation reviewed semiannually;

   5.7 virus prevention, detection, and anti-malware solutions within the Cloud-based Services, the Vertex Network, and Vertex-issued laptops, with virus signatures updated daily;

   5.8 external and internal vulnerability testing for Cloud-based Services, including annual penetration testing;

   5.9 hardening practices to protect the Vertex Network and Cloud-based Services from vulnerabilities;

   5.10 secure by design, defense in depth approach to development and maintenance of Vertex software incorporated in Cloud-based Services in accordance with a defined software development life cycle framework, including regular code review using application security and code analysis tools; and

   5.11 remediation of vulnerabilities with appropriate timelines based on severity.

6. **User Access Management.** Vertex will ensure that all access to the Vertex Network and Cloud-based Services is restricted to authorized individuals and Vertex will enable Customer to restrict Customer users' access to Cloud-based Services. These restrictions will be supported by authentication controls, including enforcement of complex password rules, consistent with industry standards, and account lockouts in all environments as well as procedures such as masking, and encryption and/or hashing, to maintain security of passwords.

7. **Network and Data Separation.** Vertex will maintain logical and physical separation between the Vertex Network and the Cloud Provider environments where Customer Data is processed and stored. Vertex's application and database security frameworks will ensure that Customer Data is logically separated from Vertex data and third-party data. Vertex will also maintain logical separation of production and non-production environments within the Vertex Network and within the Cloud-based Services.

8. **Physical and Environmental Controls.** Vertex will employ industry standard measures to manage physical security, mitigate security risks, and prevent and detect unauthorized access to Vertex facilities, systems, and assets. Vertex will equip its corporate buildings with physical access control systems such as access badge readers and monitoring, and registration systems for visitors that restrict access and track information about individuals. Vertex will also implement and regularly test fire suppression measures and environmental controls, where required for systems performance. To protect Customer Data while stored or processed using Cloud-based Services, Vertex will ensure Cloud Providers maintain physical security for their data centers using state-of-the-art controls and equipment to protect their data centers from threats and unauthorized access. Vertex will also ensure Cloud Providers enforce other controls designed to ensure redundant operations during environmental incidents, including continuity of electrical power, fire suppression, and humidity and temperature controls.

9. **Change Management.** Vertex will implement and follow formal change management processes that require software and infrastructure changes affecting the Cloud-based Services or the Vertex Network to be formally documented, tested, reviewed, and approved prior to migration to the production environment. Infrastructure and software changes are managed and tracked using work management systems. The change management processes are appropriately segregated, and access to migrate changes to production is restricted to authorized Vertex Personnel.

10. **Vendor Management.** Vertex will implement and follow formal vendor risk management processes that require documented risk assessment, with scrutiny and mitigation commensurate with the level of risk. Vertex's agreements with Cloud Providers and other key vendors involved in provisioning Cloud-based Services or the Vertex Network will include information security and data protection commitments, including where appropriate requirements to conduct, maintain, and provide on request evidence of third-party audit and/or certification according to the Service Organization Controls (SOC) reporting framework, ISO/IEC, or other similar framework or standard.

11. **Incident Response.** Vertex will maintain a documented Security Incident Response Plan. Vertex will triage, investigate, manage, and appropriately report security incidents, compromises, vulnerabilities, and concerns, including those reported by customers. The Response Plan will be reviewed and approved annually and tested annually. If Vertex becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "**Data Security Incident**"), Vertex will notify affected Vertex customers no later than twenty-four (24) hours after Vertex becomes aware of the incident, unless notification is prohibited by law. Vertex's notification will include the following information, to the extent known by Vertex:

    11.1 a description of the nature of the Data Security Incident, the types of Customer Data involved, and the number of Customer Data records involved;

    11.2 a description of the likely consequences of the Data Security Incident;

11.3 a description of the measures Vertex has taken or proposes to take in response to the Data Security Incident; and

11.4 the name and contact details of the Vertex representative who will provide additional information to affected Vertex customers on request.

Vertex will promptly supplement its initial notification with additional information learned during the incident response process that is reasonably necessary to enable affected Vertex customers to understand and assess the incident, and to meet any notification or other obligations under applicable law.

Vertex will promptly take all reasonable steps to contain and mitigate the effects of the Data Security Incident and implement appropriate controls to prevent its recurrence. Vertex will comply with applicable law in its response to the Data Security Incident. Vertex will be responsible for Data Security Incident response and investigation, and will cooperate with and assist affected Vertex customers and their representatives, law enforcement, and any data protection authority or other appropriate governmental body in connection with Vertex's response and investigation. Except for notice to law enforcement, to Vertex's incident response service providers (including Vertex's insurers), to affected Vertex customers as described in this section, and any additional notifications Vertex is required to make under applicable law, Vertex will not notify any third party or any data subject who may have been affected by a Data Security Incident.

12. **Business Continuity.** Vertex will plan for the continuation of business operations during adverse or disruptive situations, and design systems to keep the Vertex Network and Cloud-based Services and other services Vertex provides to customers operational during the occurrence of such events. Vertex's business continuity plans will be documented and will provide for redundancy of all mission-critical systems, data, and infrastructure, including backup of Customer Data to remote media and failover and mirroring processes. Vertex will review and test its business continuity plans at least annually against applicable recovery and restoration objectives.

13. **Audit.** Vertex will complete annual SOC 1, Type II and SOC 2, Type II external audits for certain Cloud-based Services and other relevant in-scope services; and Vertex will maintain ISO 27001 certification for the Information Security Management System governing operations of Vertex's EU-based Affiliates Taxamo Checkout Limited and EVAT Solutions Limited. These audit reports and certification are available upon request. Vertex will also provide written responses to all reasonable requests made by Customer for information relating to Vertex's processing of Customer Data, including responses to information and security audit questionnaires submitted by Customer and that are necessary to confirm Vertex's compliance with this Security Exhibit, provided (a) the requested information is not included in any self-assessment questionnaire that Vertex makes available, and (b) Customer shall not exercise this right more than once per calendar year or when Customer is expressly requested or required to provide this information to a data protection authority. While it is the parties' intention ordinarily to rely on Vertex's audit reports, certifications, and written responses described above to verify Vertex's compliance with this Security Exhibit and Data Protection Laws, following a confirmed Data Security Incident or where a data protection authority requires it, Customer may provide Vertex with thirty (30) days' prior written notice requesting that a third party conduct an audit of Vertex's facilities, equipment, documents, and electronic data relating to the processing of Customer Data under the Agreement ("**Audit**"), provided that: (1) the Audit shall be conducted at Customer's expense; (2) the parties shall mutually agree upon the scope, timing and duration of the Audit; and (3) the Audit shall not unreasonably impact Vertex's regular operations. Customer acknowledges that any audit report, certification, written responses, or Audit described in this section shall be subject to the confidentiality provisions of the Agreement.

Screening Attachment to Security Exhibit

Vertex's background verification and screening for Vertex Personnel will include background checks, covering the past seven (7) years (or, if shorter, the maximum period permitted by law) against such matters as would be assessed by a reasonable employer in Vertex's position in the relevant jurisdiction in which an individual is employed. Subject to applicable law, these checks may include verification of previous employment, educational history, and criminal background checks. Vertex will conduct the following checks for Vertex Personnel in the US:

(a) Widescreen Plus national criminal search: search a proprietary database of millions of criminal records, including but not limited to felonies and misdemeanors, traffic violations, and sex offender records;

(b) criminal felony and misdemeanor: perform fundamental criminal searches that reveal felonies and misdemeanors in searching county courthouse records corresponding to an applicant's address history;

(c) SSN validation: detect an incorrect or compromised Social Security Number using data from the Social Security Administration and other databases;

(d) SSN trace: reveal the names and addresses associated with the Social Security Number using credit bureau records;

(e) employment report: for not more than three (3) prior employers, verify company names and locations, dates of employment, and positions and titles held (and compensation when available); and

(f) education report: confirm degree, certificate and diploma claims directly with institutions or their authorized agents.