PRIVACY AND SECURITY

1. **Definitions.**
"**Personal Data**" has the meaning given to it in the Master Terms.
"**Personnel**" refers to Supplier's employees and consultants having access to Data or systems used to provide the SaaS Service and SaaS related Support Services under the Contract.

2. **Generalities.** Supplier shall maintain a comprehensive information security program designed to protect the security and confidentiality of Data and protect against any reasonably anticipated threats or hazards to the security or integrity of such Data.

3. **Technical and Organizational Measures and Information Security.** Supplier shall comply with the following security measures with regard to its production environment:
   3.1. Administrative Safeguards.
      3.1.1. Information Security Policies. Supplier shall have in place a comprehensive information security policy framework, including but not limited to policies and standards (herein collectively referred to as "Security Policies"), aligned with industry standard practices, as applicable. Such Security Policies shall address matters of information security and meet reasonably relevant/applicable statutory, regulatory and contractual requirements and have, as applicable, supporting guidelines, processes and procedures in place that set forth how Supplier will meet its security commitments. Security Policies shall include appropriate administrative, technological and physical safeguards to: (i) protect against threats to the security and confidentiality of Data, including unauthorized use, access or disclosure; (ii) ensure a consistent level of protection for Data during both normal operations and extraordinary circumstances, such as when Supplier is operating under a business continuity or disaster scenario; (iii) limit access to Data to those with a "need to know"; and (iv) ensure the secure disposal of Data. Security Policies shall be approved by senior management, communicated to Personnel and reviewed on an annual basis to ensure accuracy and completeness, and to take into account changing standards and evolving threats and hazards. Security Policies shall have provisions for disciplinary measures in case of violation.
      3.1.2. Confidentiality. Personnel, contractors and consultants shall be subject to obligations of confidentiality which meet the intent of those found in this Contract.
      3.1.3. Personnel security. Personnel shall have clearly defined job descriptions that include security requirements and responsibilities and such job descriptions shall be reviewed periodically to ensure their accuracy and completeness. Personnel shall undergo a background check to the extent permitted by applicable law, which includes, but is not limited to, identity verification, a criminal record check, past employment verification, education records verification, reference checks, as well as screening against the Office of Foreign Assets Controls of the U.S. Department of the Treasury's "Specially Designated Nationals List". Personnel shall sign a non-disclosure agreement. Personnel shall also, on a yearly basis, sign a "Privileged User Agreement" or similar form, and acknowledge the Company's Code of Conduct. Personnel shall attend Code of Conduct training and Information Security and Privacy Awareness sessions on an annual basis.
      3.1.4. Access control. Supplier shall maintain procedures and controls to authenticate and limit access to the systems used to provide the SaaS Service to authorized individuals. Access to such systems shall be granted on a need-to- know basis, applying the least privilege principle, as applicable. Personnel with administrative privileges shall be required to use multifactor authentication in order to get access to such systems. Personnel shall not access or view any Data unless required to provide the SaaS Services under the Contract. Access shall be removed promptly upon termination, or upon position change, as required.
      3.1.5. Risk management. Supplier shall have in place a process to and conduct regular and comprehensive assessments of reasonably foreseeable internal and external risks and vulnerabilities to the confidentiality, integrity and availability of Data that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such Data, and design and implement safeguards to reduce these risks and vulnerabilities to a reasonable and appropriate level.
      3.1.6. Change management. Supplier shall have in place a formalized change management process which requires the identification, documentation, testing, approval and post-implementation review of application and infrastructure changes that may impact system security, stability, availability or otherwise have an adverse effect on the SaaS Service. Proposed changes shall be evaluated to determine if they present a security risk and what mitigating actions must be performed. Access to production systems shall be strictly limited and developers shall not have the ability to migrate changes into the production environment.
      3.1.7. Incident management. Supplier shall have in place an incident management framework designed to respond quickly and efficiently to all types of internal and external security and operational events that threaten the

confidentiality, integrity or availability of the system used to provide the SaaS Services and any Data contained therein.

3.1.8. Business continuity and disaster recovery. The SaaS Service shall be designed with the resources reasonably necessary to support availability of the SaaS Services in accordance with the Service Levels, and in a way that would enable recovery within the established Recovery Time Objective (RTO) following a service interruption. Testing of necessary components shall be performed as reasonably required to ensure recoverability.

3.1.9. Organizational audits. At least annually during the Term, Supplier shall have, at its sole expense, a reputable qualified third party conduct a Service Organization Control (SOC) 2 assessment of the SaaS Service to assess the suitability of the design and the operating effectiveness of the controls to meet the Trust Services Principles and Criteria for Security established by CPA Canada/AICPA's TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids). Such assessment shall reasonably cover all sites being used to provide the SaaS Service, herein referred to as an "Organizational Audit". In addition to including a description and assessment of the controls in place, the Organizational Audit report will also include a description of organizational, operational and business controls relating to the SaaS Service, within the general framework of the type of Organizational Audit in question. Supplier shall make available to Customer a copy of the SOC 2 report summarizing the findings of such Organizational Audit, upon written request.

3.2. Technical Safeguards.

3.2.1. Data segregation. Supplier shall ensure that Data is stored, used, accessed and disposed of in a secure environment, and logically segregated at all times from its other clients' data, including when operating under a business continuity or disaster recovery scenario.

3.2.2. System configuration. The system used to provide the SaaS Service shall be segmented into separate network zones protected by firewalls or equivalent mechanisms to mitigate the risk of unauthorized access and to stop the spread of malware infections at internal and external access points. Supplier shall maintain procedures and controls for the secure installation, configuration, operation and maintenance of information systems (e.g., workstations, servers, networks and applications), including procedures for change management, patch management and vulnerability management. System components shall be configured according to hardening guidelines and feature antivirus and intrusion detection systems, as applicable.

3.2.3. Application development. Supplier shall use separate environments for the purposes of development, testing, staging and production, so that any changes to infrastructure and software are developed and tested in a separate environment before being implemented into production, and to reduce risk of inadvertent changes to a production environment. Supplier shall perform code reviews and analyses of its software on a regular basis to reduce the likelihood of any vulnerability being deployed into production.

3.2.4. Monitoring. Supplier shall maintain procedures and controls for detecting, preventing and responding to attacks, intrusions or other systems failures, including actions to be taken in the event of suspected or detected unauthorized access to Data. Supplier shall have in place and maintain tools, including but not limited to a Security Incident and Event Management (SIEM) system, to allow for appropriate ongoing monitoring of the health and security of the SaaS Service, including the detection of possible security threats and incidents. Such tools shall monitor system availability, resource usage, security events, unauthorized system changes and unusual activity, and have automated notifications for system and security issues in real time. Monitored events shall be correlated centrally and event logs shall be reviewed regularly to allow for prompt identification of issues, for capacity planning and for appropriate action to be taken in a timely period in respect of any issues detected from such reviews.

3.2.5. Vulnerability management. In order to identify potential SaaS Service vulnerabilities, Supplier shall conduct vulnerability assessments on a regular basis. Such assessments shall include application vulnerability testing. Security patches and updates shall be applied as required according to their criticality.

3.2.6. Security Testing. At least annually, or aligned with delivery of major releases, and at Supplier's sole discretion, Supplier shall retain a qualified, reputable third party to perform penetration testing of the SaaS Service and to prepare a report of its findings.

3.2.7. Use of encryption. Supplier shall use appropriate encryption, using industry-accepted algorithms and key lengths, to protect Data stored in the SaaS Service, or transmitted over public networks, in connection with the SaaS Services.

3.2.8. Use of portable storage. Unless explicitly requested by Customer or required to provide SaaS Services under this Contract, and protected by encryption, Data shall not be copied onto computer systems or media not permanently housed in secure Hosting Facilities (including laptop computers, portable storage devices or removable media such as USB disks, DVDs and tapes).

3.3. Physical and Environmental Safeguards. Access to areas at a Supplier site from which the SaaS Service is managed and can be accessed shall be physically restricted to authorized Personnel only, and controlled through the use of access badges. Visitors and third parties shall only be allowed to access to such Supplier work area once they have been properly identified and authorized.

3.4. Hosting Facilities

3.4.1. Supplier shall host equipment used to provide the SaaS Services in a physically secure area with access restricted to authorized personnel, herein referred to as "Hosting Facilities". Hosting Facilities shall have adequate physical security measures such as, but not limited to, perimeter controls which include a provision to detect unauthorized access, access logging, strong authentication, video surveillance and visitor sign-in.

3.4.2. Hosting Facilities shall be reasonably protected against external/environmental threats such as fire, flood or other forms of natural or man-made disasters. Protection measures shall include controls such as smoke and fire detection alarm systems and/or automatic fire suppression systems.

3.4.3. Hosting Facilities shall have protection in place for servers, network and other electronic equipment against power related problems.

3.4.4. Supplier shall periodically review the physical and environmental controls to ensure they remain adequate to host the equipment used to provide the SaaS Services.

3.4.5. Where any hardware or media is no longer being used to provide the SaaS Services, Supplier or its subcontractor will promptly render irrecoverable any Data on that hardware or media, as applicable.

4. Privacy Requirements

4.1. Access and Correction Requests. Supplier will refer to Customer all access or correction requests from Data Subjects (as defined in the Customer Data Processing Addendum) for Personal Data and reasonably cooperate with Customer in its response to those requests, as required under applicable Data Protection Law (as defined in the Customer Data Processing Addendum).

4.2. Breach Notification and Investigation. In the event that Supplier becomes aware that the security, confidentiality or integrity of any Data has been compromised("Data Breach"), Supplier shall use commercially reasonable efforts to immediately, in writing, in accordance with the notice requirements set out in the Contract, but in no event more than two (2) business days (where feasible) following discovery or notification of such Data Breach, report to Customer and, if required by law or regulation, to any other party. Supplier shall also (i) promptly investigate and conduct a reasonable analysis of the cause(s) of the Data Breach, (ii) to the extent such cause is within Supplier's control, develop and implement an appropriate plan to limit the effect and remediate the cause of the Data Breach; and (iii) reasonably cooperate with Customer in respect of any investigation and/or efforts to comply with any notification or other regulatory requirements applicable to the Data Breach. Subject to any confidentiality and/or contractual agreements Supplier may have with other parties, Supplier will give Customer any information Customer reasonably requests about the incident.

4.3. Data Protection Officer. (DPO). To facilitate compliance with applicable data protection law Supplier has engaged a qualified independent external data protection officer. The DPO oversees Supplier's compliance with its data protection obligations under this Contract and acts as Customer's primary point of contact for privacy matters. The DPO's contact information is to be found on the OneSpan Privacy Center (https://www.onespan.com/privacy-center) under "Privacy Highlights" – Data Protection Officer.

4.4. Supplier has appointed a Chief Information Security Officer who oversees the Supplier's compliance with information security obligations under this Contract and acts as the Customer's primary point of contact for information security matters. More information can be found under the Security Highlights on the OneSpan Privacy Center (https://www.onespan.com/privacy-center).