opentext™
Information reimagined

Information Security
Terms and Conditions

Supplier shall comply with the Information Security Terms and Conditions set forth in this document and ensure any subcontractor engaged by Supplier at any tier complies with this document. For the purposes of this document, "**OpenText Data**" means any data, whether electronic or otherwise, personal or not personal belonging to OpenText that Supplier may collect, access, use, host, store, process, or transmit including, without limitation, any data specifically pertaining to company, its affiliates, or its employees, users, partners, customers, or suppliers.

1 Organizational Security

1.1 Compliance

a) **Supplier System Security Requirements:** For all systems used by Supplier to collect, access, use, host, store, process or transmit OpenText Data, Supplier shall comply with at least SSAE18 SOC2 or ISO27001 security standards. OpenText may require additional security standards including, but are not limited to, SSAE18 SOC1, SOC2, PCI-DSS, or HIPAA/HITRUST standards.

b) **Annual Compliance Audit and Reporting**: On an annual basis, Supplier shall provide or make available within five (5) business days of receipt of a written request from OT, the Supplier shall provide a current independent audit report (e.g. SSAE18 SOC1, SOC2, SOC3, ISO27001, PCI-DSS) that validates the security compliance controls of those systems.

c) **Information Security Assessment:** Upon request, Supplier shall complete an annual information security assessment questionnaire supplied by OpenText, at no additional cost.

1.2 Right To Audit

a) **Security Audit**: Within five (5) business days of receipt of a written request from OpenText, Supplier shall:
   - provide OpenText with reasonable access to its personnel, premises, facilities and subcontractors to enable OpenText to conduct an on-site inspection audit, provided that any on-site audit shall be conducted during ordinary business hours on business days and shall not interfere unreasonably with Supplier's ordinary business; and
   - provide evidence of Supplier's relevant policies and other related documents to verify that Supplier is complying with its obligations under these Information Security Terms and Conditions. Any audit shall be conducted, and all information to be provided pursuant to this clause shall be provided, at the cost of the Supplier. Examples of a right to audit may include data breach, major changes to the service being provided, supplier may have gone through an M&A.

b) **Audit Findings Remediation**: If the results of an audit show that Supplier is not complying with these Information Security Terms and Conditions, then Supplier must ensure prompt remedy of the non-compliance under a remediation plan and comply with OpenText's reasonable directions to remedy the non-compliance, including without limitation directions as to timing. If the remediation plan does not adequately address any deficiencies to OpenText's satisfaction, OpenText reserves the right to terminate the Agreement at its sole discretion.

c) **Regulatory Audits:** Under applicable laws or regulations, OpenText and its customers must meet certain additional security audit, business continuity, disaster recovery, and data protection requirements ("**Regulatory Requirements**"). As required in order to comply with a Regulatory Requirement, Supplier will allow on-site audits by competent supervising body having jurisdiction under such Regulatory Requirement and representatives of OpenText's customer being subject to such Regulatory Requirement.

d) **Audit Logs:** Supplier shall ensure all system log information is stored in a centralized location. Logs will be retained for at least one (1) year and protected from unauthorized changes or deletion. They will be backed

up daily and monitored for risks and anomalies. Logs shall be made available during a security audit or security incident.

1.3 Information Security Roles and Responsibilities

a) **Security Point of Contact:** The Supplier shall designate an Information Security Officer or designated representative to serve as the primary point of contact for OpenText for the duration of the Agreement. This point of contact shall be responsible for coordinating and communicating with an OpenText Information Security Officer on all security-related matters.

1.4 Access Controls

a) **Access Management:** Supplier shall maintain an up-to-date list of any employees and subcontractors ("**Representatives**") accessing OpenText Data at all times.
b) **Granting Access:** Supplier shall ensure and document that access to OpenText Data is granted according to principle of least privilege.
c) **Access Termination:** Supplier shall ensure that a process for termination of all types of access including account termination is in place.
d) **Access Audit:** Supplier shall, at least on an annual basis or other such frequency, ensure and document that logical access is reviewed for need and that unused accounts including privileged and service accounts are removed.
e) **Segregation of Duties:** Supplier shall separate conflicting duties on systems and accounts processing OpenText data to reduce risk of error or fraud.
f) **Malicious Intent Termination:** Supplier shall immediately remove all logical and physical access to all Supplier systems of any Representative who was found to have or suspected or potential to have malicious intent to harm OpenText Data.
g) **Change Of Employment:** If a Supplier employee is due to have a change of employment or a subcontract is to be terminated, all access is to be removed on or prior to the date and time of termination.

1.5 Information Security Incident Management

a) **Security Incident Planning and Preparation:** Supplier shall create and adhere to a formally documented security incident management response plan. Incident management process shall include the process to remediate a ransomware attack.
b) **Data Breach Notification:** Supplier shall immediately notify OpenText (but no less than within 24 hours) of a Data Breach. OpenText shall be notified via email at reportsecurityincident@opentext.com. A "**Data Breach**" refers to a suspected security incident or breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, OpenText Data.
c) **Security Incident Cooperation and Remediation:** Supplier shall cooperate with OpenText personnel in the diagnosis, investigation and correction of any Data Breach. Remediation steps shall be taken as soon as the Data Breach has been detected. Supplier shall provide consistent updates and remediation steps to OpenText when prompted by OpenText. Supplier shall provide steps to avoid recurrence of the Data Breach and provide an incident impact assessment identifying its root cause.

1.6 Business Continuity

a) **Business Continuity Plan:** Supplier shall have business continuity and disaster recovery plans and processes in place to ensure the service for OpenText is adequately maintained in the event of any negative impact on Supplier's service.
b) **Data Recovery:** Supplier shall regularly backup OpenText Data and retain such backup data copies for a minimum of twelve (12) months.

c) **Testing Business Continuity:** Supplier shall conduct at least an annual testing of Supplier's Business Continuity Plan and provide a copy of the Business Continuity Plan and the results of such test to OpenText upon request.

2 People Security

2.1 Screening Supplier Personnel

a) **Background Checks:** Supplier shall carry out necessary background verification checks of all its Representatives during onboarding or granting any potential access to OpenText Data. Background checks, at a minimum, shall include a criminal check, employment verification, and education verification. To the extent permitted under applicable laws, OpenText may require additional background check requirements as required to comply with contractual requirements with its customers.

2.2 Information Security Training

a) **Information Security Training and Confidentiality:** The Supplier shall ensure that all Representatives involved in the processing of OpenText Data are fully informed of and understand the security policies implemented by Supplier, which policies shall at least comply with these Information Security Terms and Conditions. Supplier is responsible for tracking and verifying that all employees and subcontractors are aware of and comply with all relevant Supplier security policies. Additionally, the Supplier shall at least annually train all Representatives on information security tailored to the specific roles and responsibilities of each Representative.

2.3 Confidentiality or Non-Disclosure Agreements

a) **Non-Disclosure:** Before granting access to any OpenText Data or to Supplier's assets hosting/storing OpenText Data, all Representatives shall be bound by a binding confidentiality agreement.

3 Physical Security

a) **Physical Security Perimeter:** Supplier shall ensure that all OpenText Data or Supplier assets hosting/storing OpenText Data are stored in a secure location that is protected by industry best standard physical protection controls. These controls include but are not limited to: physical entry, securing offices, rooms and facilities, physical security monitoring, security of assets off-premises, storage media.

4 Technological Security

4.1 Assets Security and End Point Devices

a) **Asset Management:** Supplier shall document where OpenText's Data and assets are hosted and provide OpenText with any information relating to the hosting location upon request.
b) **Information Technology Process:** Supplier shall provide OpenText documentation relating to its information technology process.
c) **End Point Malware Security:** Supplier shall enforce end-point security on all assets that connect to OpenText infrastructure, including encrypted connectivity and anti-virus/anti-malware software.
d) **Asset Access:** Upon request, Supplier shall be able to provide evidence of all Supplier assets accessing OpenText Data.

e) **Vulnerability Detection and Remediation:** Supplier shall establish a vulnerability detection and management process, and software patch management process on all its assets accessing OpenText Data.
f) **Use of Multi-Factor Authentication:** Supplier shall implement and enforce multi-factor authentication (MFA) for all personnel, subcontractors, and third parties accessing any systems, applications, or data related to or used. MFA requires at least two independent verification methods (such as a password plus a device code, biometric factor, or hardware token) for authentication to all relevant systems, including administrative, user, and remote access accounts.

4.2 Network and Application Security

a) **Network Scanning:** Supplier shall perform periodic internal and external (but no less than once per month) network vulnerability scan on all infrastructure components of its production and development environment. A summary report of the network vulnerability scan results shall be provided to OpenText upon request.
b) **External Application Penetration Testing:** An application penetration test must be performed reputable third-party provider on an annual basis, on any internet facing applications being used in the Supplier's products or services. Upon request, Supplier shall provide OpenText with summary results of the penetration test relating to any Supplier services processing OpenText Data, at no cost.
c) **Application Code Scanning:** Supplier shall perform periodic (but no less than once per quarter, as well as after making any change to the Supplier systems processing OpenText Data) application scan on in-scope systems that process OpenText Data.
d) **Remediation Of Vulnerabilities:** Vulnerabilities shall be remediated on a risk basis. Supplier shall install all Medium, High, and Critical security patches for all components in their production and development environment as soon as commercially possible. Supplier shall promptly address any issues, retest, and provide a new report to OpenText. OpenText may share these reports with its customers for whom Supplier processes information or provides maintenance/support services.
e) **Data And Network Segregation:** Supplier shall use physical and logical controls to segregate OpenText Data from that of other customers. Upon request, Supplier shall produce documentation describing data segregation controls to OpenText.

4.3 Cryptography

a) **Use Of Cryptography:** Supplier shall use current industry-best standard encryption methods to protect OpenText Data both during transfer and at rest. This includes encrypting data during transit between servers and end points, as well as encrypting stored data, including on mobile devices. Supplier shall ensure proper encryption for data transfer within secured networks. Additionally, Supplier shall have a defined encryption key management policy covering key creation, rotation, and destruction.

4.4 Change Management

a) **Approval For Change:** Supplier shall not alter, adapt or change any OpenText's systems that Supplier may have access to without OpenText approval.
b) **Change Management Process:** To the extent applicable to the contract, Supplier shall adhere to a documented change management process that protects changes to OpenText Data or OpenText environments as applicable.

4.5 Data Destruction and Information Deletion

a) Upon termination of the Agreement, Supplier shall immediately return all OpenText Data and OpenText assets to OpenText or, at OpenText's sole discretion, destroy all OpenText Data. If OpenText requests that OpenText Data be destroyed, NIST SP 800-88 or Department of Defense 5220.22-M methodology shall be used, and Supplier shall provide OpenText with a certificate of destruction.