

Technical and Organizational Measures

These Technical and Organizational Measures are attached to and form part of the agreement between the parties that references this document expressly (“Agreement”). Unless otherwise defined in this attachment, capitalized terms used in this attachment have the meanings given to them in the Agreement. Where the Technical Organizational Measures are attached as part of the Agreement, the controls stated below are only applicable as specified for the services in the Agreement.

For clarity, these measures do not apply where the customer is responsible for security and privacy either at law or as stated below or in the Agreement. Customer is responsible for implementing and managing security and privacy measures for components that OpenText does not provide as part of OpenText services. Customer is also responsible for determining whether the OpenText services are suitable for its use.

Technical and organizational Measures

This document describes the technical and organizational security measures implemented by OpenText to ensure a level of security appropriate to protect customer data.

OpenText may implement changes to these measures from time to time without prior notice, provided such changes do not result in a material degradation of the overall level of security for customer data.

This document outlines OpenText’s current technical and organizational measures that apply to OpenText to the extent it processes customer data in connection with the performance of the Agreement in general and to the OpenText’s production systems – when applicable- which may operate either in OpenText’s own infrastructure or in cases involving any third-party cloud infrastructure (OpenText Production Systems) where a subset of the measures detailed above applies.

Physical Access Control

This control describes the measures to regulate access to OpenText Production Systems where customer data is hosted or stored. OpenText ensures that data centers used in the delivery of the OpenText services meet the following minimum standards. Additional information about the physical access controls applied by third-party cloud infrastructure providers or any other third party engaged by OpenText can be obtained upon request.

Data center facilities are designed to physically protect equipment and other critical resources from unauthorized access and environmental hazards. The data centers where processing, storage and communication equipment are installed are protected with the following security measures:

- a) On-site security guards’ control and monitor access to the data centers 24 hours a day, 7 days per week.

- b) Physical access control systems (including, but not limited to, named access lists, badge readers, physical keys and/or biometric controls) are installed at entry points to the data center and areas within the data center to restrict access. Personnel must pass an area where they are observed by security company personnel and access to the data center through a circle lock/mantrap to prevent tailgating.
- c) Within the data center, sensitive areas are separated and are only accessible to personnel by use of their personal access control credentials, with the required privileges granted on a need-to-know basis and a legitimate business need approved by management.
- d) Technical facility rooms are locked, and access control credentials are kept on site with issuance registration.
- e) Emergency exterior doors trigger an audible alarm when opened.
- f) Third-party visitors and deliveries must be pre-announced, with access approved by listed approvers and visitors are escorted in the data center.
- g) A secure intermediate holding area is used for all deliveries. Delivery personnel do not have direct access to areas containing computer systems or communication facilities.
- h) CCTV (video) surveillance and motion detection equipment is installed at key points in the facilities, including but not limited to, parking lots, reception areas and data center rooms. Recordings are retained in line with applicable data privacy regulations.
- i) Access is monitored by guard station personnel. Access reports and access privileges are reviewed by management.

System Access Control

This control describes the measures to prevent unauthorized logical access to OpenText Production Systems. Additional information about the system access controls applied by third-party cloud infrastructure providers or any other third party engaged by OpenText can be obtained upon request.

Production Systems and networks have logical access controls in place and are segregated from corporate and public networks. Employee access rights are granted following the least privilege access principle, on a need-to-know basis and with legitimate business need. All access requests are validated by the information security personnel and approved by management. System authentication credentials assigned to individual OpenText personnel are solely for their own use. Authentication credentials must not be shared or disclosed to any third party. It is a breach of policy for any user to misuse their or other users' authentication credentials.

Passwords must comply with the password policy published in the Information Security Policy in terms of complexity which, as of the effective date of this document, are:

- a) A 10-character minimum password must be utilized where supported.

- b) Where system constraints exist, the maximum character length supported by the system configuration capabilities must be utilized.
- c) Passwords must contain at least one alpha character in upper case, one in lower case, one numeric and one non-alphanumeric character.
- a) And the following thresholds apply to OpenText corporate accounts: Personal accounts will lock after six consecutive failed login attempts.
- b) Personal accounts that are not utilized within 90 days will automatically become disabled.
- c) Passwords for user accounts must be changed after their initial creation.

For access to production environments by OpenText personnel, secure logical access gates are in place and require multi-factor authentication. Recording of activities on production systems is done through logging and using software deployed on the access gates.

Regular validation of access privileges is performed by information security personnel and functional managers to control moves, adds or changes to privileges and accounts.

The OpenText Information Security Group maintains a centrally managed and monitored Universal Threat Management (UTM) solution in place, which has Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) capabilities.

Select facilities support data at rest encryption using Advanced Encryption System (AES) or greater.

Data Access Control

This control describes the measures to prevent data being read, copied, modified or deleted without authorization in OpenText Production Systems. Additional information about the data access controls applied by third-party cloud infrastructure providers or any other third parties engaged by OpenText can be obtained upon request.

In addition to the Physical and System Access Controls described above, access to customer data is stored within a secured environment. Access controls are enforced based on least privilege and multi-factor authentication for production environments. Access reviews are conducted periodically, and unused accounts are disabled within a commercially reasonable timeframe. Segregation of duties is enforced across administration, deployment and change approval roles.

All production systems are operated in secure data centers or facilities. Security measures that protect systems processing customer data are regularly checked. To this end, OpenText conducts regular internal and external security checks and penetration testing on its data processing infrastructure.

Installation of software on the OpenText network is subject to approval by the OpenText Global Information Security group.

Disclosure Control

This control ensures that the confidentiality of customer data is protected from unauthorized disclosure during processing, transmission, and storage by utilizing our multi-layer/defense in depth security approach for OpenText Production Systems. Additional information regarding the disclosure controls applied by third-party cloud infrastructure providers or other third parties engaged by OpenText is available upon request.

A multi-layer security approach depends on maintaining appropriate security measures and procedures at five different levels within the production environment:

Perimeter

- a) Perimeter firewall
- b) Distributed Denial of Services (DOS) protections (in select facilities)
- c) Private IP connection with customers is available for order by customers on a case-by-case basis

Network

- a) Intrusion Detection System (IDS)/Intrusions Prevention System (IPS)
- b) Vulnerability management system, both vulnerability scans and third-party penetration testing
- c) Access control/User authentication, multi-factor authentication for access to the production environment
- d) Load Balancer/VLAN filter deployment to control network access

Host

- a) Hosts and virtual servers are hardened, including thread and Vulnerability Assessments
- b) Load Balancer/VLAN filter deployment to control network access
- c) Anti-virus/Anti-malware protections
- d) Access control and user authentication

Application

- a) Access control and user authentication

Data

- a) Encryption of data in transit and data at rest (as set out in the Agreement)
- b) Access control/user authentication
- c) Shielded (secured) replication to remote site for Disaster Recovery synchronization

OpenText networks and service environments are isolated from foreign networks. Network routers and switches are configured with strict access control lists to prevent uncontrolled routing and broadcasting of network routes. Firewalls are configured with ingress and egress filters and only allow access to select services on the multi layered production systems and networks.

OpenText implements a vulnerability management program that includes periodic scanning, penetration testing and code analysis for applicable production systems. OpenText endeavors to remediate identified

vulnerabilities based on severity within commercially reasonable timeframes, subject to operational constraints.

To protect data in transit and provide secure communication in transit, inherent encryption is applied based on transmission protocol. End-user sessions from their browser to portal applications are encrypted with HTTPS by policy. OpenText maintains a Key Management Policy addressing lifecycle practices covering key generation, rotation, storage, access controls, separation of duties, and secure destruction.

Disposal of redundant processing and storage equipment or media is accomplished following strict disposal procedures that include the use of certified data destruction processes and/or companies. OpenText removes all copies and instances of customer data from OpenText's disk storage, backups and archives per NIST 800-88 or Department of Defense 5220.22-M standard protocols. Upon request, OpenText will certify in writing that all customer data has been removed in line with these protocols subject to technical and contractual constraints (e.g., third-party cloud provider timelines) as applicable.

Input Control

Input control enables verification of when, where and by whom customer data in the OpenText Production Systems has been entered, edited or deleted. Additional information about input-related controls applied by third-party cloud infrastructure providers or any other third party engaged by OpenText can be obtained upon request

All access to information and systems by OpenText personnel is enforced through a least privileged access policy, a full, role-based, lifecycle for identity access management process and a regular cadence review and validation of all access privileges. Workforce members are only granted rights to access assets needed to fulfill job functions.

Change Control

All system changes must be recorded, verified, tested and approved following a change management process that is based on the Information Technology Infrastructure Library (ITIL) standard.

Availability Control

Through this control, the accidental destruction or loss of customer data is protected.

Data center facilities are designed to physically protect equipment and other critical resources from unauthorized access and environmental hazards. data centers are designed to meet industry standards and practices. All critical technical facilities such as power, cooling and networking are redundant with A+B feeds. The systems are proactively monitored 24 hours a day, 7 days a week.

OpenText maintains documented business continuity and disaster recovery plans with defined objectives. OpenText conducts periodic testing and may provide summaries upon request.

OpenText performs regular risk assessments and recovery tests on at least an annual basis covering its business processes, systems or applications as appropriate

Data Segregation

Data collected for different purposes can be processed separately.

To ensure that data collected for different purposes can be processed separately, OpenText segregates its corporate and commercial operating environments. No data from the commercial production environment is permitted in the OpenText corporate environment unless explicitly approved in limited circumstances defined by OpenText policy.

Access from the corporate to commercial networks is provided through security gates that require multi-factor authentication, perform logging and whose access is provisioned via the centrally authorized Global Information Security Unit.

Data storage is logically segregated customer-by-customer with partitioning. All data segregation by tenant is engineered to ensure data is not commingled.

Security Incidents management and notification

This control describes the measures implemented by OpenText, in its role as the service provider, for managing and responding to Security Incidents.

OpenText policies follow NIST Computer Security Incident Handling Guide - preparation, detection and analysis, containment eradication & recovery and post incident activity (or equivalent industry practices) to monitor, detect and respond to a Security Incident. A "Security Incident" means a confirmed security breach leading to an unauthorized access, use, destruction, loss or alteration of customer data. The OpenText process ensures that appropriate steps are taken and information is documented in the event of a Security Incident.

OpenText will notify the customer without undue delay of any Security Incident that impacts the customer data. OpenText will provide the customer with reasonably requested information about the Security Incident.

If the customer suspects a vulnerability or incident, it can submit its concerns to OpenText via the incident reporting process, or as a technical support request.

Logging & Monitoring

This control applies to OpenText Production Systems. Additional information about logging and monitoring controls applied by third-party cloud infrastructure providers or other third parties engaged by OpenText is available upon request.

OpenText maintains centralized logging for security-relevant events including access to the Cloud Environment and administrative actions within the Support platform and endeavors to retain such logs for a commercially reasonable period. Logs are monitored for anomalies. Logging and monitoring of assets and user activity and alerts for malicious or anomalous events reviewed by Security Operations Centre (SOC).

Certifications & Compliance

This control describes the measures implemented by OpenText, as the service provider, to maintain compliance with recognized security and privacy standards. Additional information about certifications or compliance attestations maintained by third-party providers engaged by OpenText is available upon request.

OpenText maintains an Information Security Management System designed to comply with recognized industry standards such as ISO/IEC 27001 and undergoes periodic audits, including SOC 2 Type II assessments for applicable services. Upon written request and subject to confidentiality obligations, OpenText may provide summaries of relevant certifications or audit reports where available or a standard security questionnaire.

Personnel Security, Training and Awareness

This control describes the measures implemented by OpenText, as the service provider, to ensure that personnel with access to information systems and customer data are trustworthy, appropriately qualified, and aware of their security responsibilities. Additional information about personnel-related controls applied by third-party providers engaged by OpenText is available upon request.

OpenText takes appropriate measures to implement personnel security and information security awareness aimed at ensuring that individuals with access to information systems and data are trustworthy, appropriately qualified, and aware of their security responsibilities.

OpenText ensures that personnel who access, process, or manage customer data receive information security training and ongoing awareness communications regularly. Such training includes awareness of information security responsibilities, data protection obligations, and applicable policies and procedures.

Personnel are trained to recognize potential security incidents and are instructed on how to report suspected incidents or vulnerabilities through established internal reporting channels.

When personnel change roles or leave OpenText, access rights are reviewed and revoked as appropriate. Offboarding procedures include timely removal of system access, return of assets, and reminders of ongoing confidentiality and data protection obligations.

Third-Party Providers

This section describes the technical and organizational measures OpenText applies to assess and govern third-party providers involved in the processing of customer data in the performance of the contract in general, including in the context of customer support or professional services when applicable. Such processing may occur on systems or tools that are distinct from OpenText Production Systems

Where customer data is processed using third-party cloud platforms or SaaS tools, such processing operates under a shared responsibility model, as OpenText does not operate or control the underlying infrastructure of those platforms. In these cases, OpenText relies on vendor security controls, contractual safeguards, and structured security due-diligence activities to ensure that the protection of customer data remains consistent with OpenText's compliance obligations, including:

- restricted access for authorized OpenText personnel using vendor-provided access controls and authentication mechanisms;
- logical data separation and confidentiality through vendor tenancy models and encryption;
- vendor-provided logging, monitoring, and audit capabilities;
- vendor change management, availability, backup, and business continuity practices; and
- vendor incident detection and response processes, with customer notification by OpenText without undue delay upon confirmation of impact to customer data.

OpenText maintains a robust third-party risk management framework designed to ensure that all vendors apply security and privacy controls proportionate to the nature of the services they provide and the level of risk involved. Each prospective vendor undergoes a thorough evaluation to confirm that they meet and will continue to meet OpenText's requirements for confidentiality, security, and data protection throughout the duration of the engagement.

Vendors that handle customer data are subject to enhanced technical and organizational safeguards. These measures are (a) formalized within OpenText's contractual terms and (b) periodically assessed by OpenText to verify ongoing compliance. In addition, OpenText conducts regular reviews of (i) each vendor's alignment with OpenText's security, privacy, and business continuity standards; (ii) the vendor's access to customer data and the adequacy of its protective controls; and (iii) evolving legal, regulatory, and industry requirements that may affect OpenText's security posture or data-processing activities.