opentext™

The Information Company

IT Security Terms and Conditions

Supplier must comply with the IT Security Terms and Conditions set forth in this document and ensure any subcontractor engaged by the supplier, also complies with the IT Security Terms and Conditions.

Compliance

- For all supplier systems used to host, store, process or transmit OpenText information, supplier must provide, on an annual basis, an independent audit report (SOC1, SOC2, SOC3, ISO27001, PCI-DSS) that validates the security controls of those systems.
- Additionally, upon request, the supplier must agree to complete an annual information security assessment questionnaire supplied by OpenText.
- For all supplier systems used to store, process or transmit OpenText information, OpenText retains the right to perform a security assessment once a year. Such Assessment may include examination of supplier's relevant facilities and records as may be reasonably required to undertake verification that supplier is complying with its security obligations. The assessment will be conducted at a mutually agreed time with no less than 30 days' advance notification, shall be limited to no more than two (2) business days and shall not unreasonably disrupt Supplier's day-to-day business operations
- In case supplier security and data protection measures do not meet (i) these terms and conditions; (ii) reasonable industry standards and / or (iii) regulatory requirements, supplier and OpenText will mutually agree a remediation plan. In case the remediation plan cannot address the findings to the satisfaction of OpenText, OpenText at its sole discretion may terminate the contract between the parties.

Organization of information security

- Supplier must make available upon request, an Information Security point of contact for the duration of the relationship defined in the contract.
- The Information Security point of contact must be responsible to liaise with OpenText Information Security Officer on all matters relating to security.

Human resource security

- Supplier must communicate information security policies to all personnel involved in work on behalf of OpenText or with access to OpenText data and track that personnel are aware of all security policies.
- Supplier shall regularly train all personnel on information security and privacy matters relevant to the nature of their function.
- Supplier personnel shall be bound by a binding confidentiality agreement before access is granted to any OpenText data or assets.

Physical and environmental security

- Supplier must ensure that all OpenText data or assets are stored in a secure location that is protected by industry standard physical protection controls.

Operational procedures and responsibilities

- Supplier must document where OpenText's data and assets are hosted and provide OpenText with appropriate documentation of the hosting location upon request.
- Supplier must not use artificial intelligence in the performance of services for OpenText which involve the analysis or processing of data of OpenText or its customers without the prior approval of OpenText.
- Supplier must provide to OpenText documentation about their Information Technology processes.
- Supplier must not alter, adapt or modify OpenText's systems without OpenText approval.
- To the extent applicable to the contract, supplier must adhere to a documented Change Management process that protects changes to OpenText data or OpenText environments as applicable.
- Supplier must enforce end-point security on assets that connect to OpenText infrastructure including encrypted connectivity and anti-virus/anti-malware software.
- Supplier must establish a vulnerability detection and management process, and software patch management process on assets accessing OpenText data.
- A network vulnerability scan of the in-scope systems must be performed by a reputable third-party provider on annual basis. A summary report of the scan results must be provided to OpenText upon request.
- A formal 3rd party application penetration test must be performed by a reputable third-party provider on annual basis, on any internet facing applications being used in the supplier's solution.
- If OpenText terminates the contract, supplier must immediately transfer all data and OpenText assets to OpenText or, at OpenText's sole discretion, destroy all data when no longer required. If data is to be destroyed, an approved methodology must be used and the supplier must provide OpenText with a certificate of destruction.
- Upon request, supplier must provide OpenText with information on roles and responsibilities of individuals that have access to OpenText data.

- Upon request, supplier must be able to provide evidence of auditing of any systems accessing OpenText data.
- Supplier must not record any conversation conducted with any OpenText personnel unless specifically agreed upon by both parties.

Access control

- Supplier must maintain an up-to-date list of employees and third parties accessing OpenText data, infrastructure, or information at all times.
- Supplier must ensure that a process for termination of personnel including account termination is in place.
- Supplier must ensure and document that access to OpenText information is granted according to principle of least privilege.
- Supplier must, on an annual basis or other such frequency, ensure and document that logical accesses are reviewed for need and that unused accounts are removed.

Information security incident management

- Supplier must adhere to a formally documented incident management process.
- Supplier must cooperate with OpenText personnel in the diagnosis, investigation, and correction of any security incidents or faults that impact OpenText data.
- Supplier must notify OpenText within 24 hours of suspicion, detection or confirmation of a breach or unauthorized access to OpenText information that is hosted/transacted or managed by the supplier, or to provide recommended protocol changes to prevent the aforementioned. OpenText Cyber Security team can be notified via reportsecurityincident@opentext.com. Supplier must include the following details:
    - Background of the security incident.
    - How was the security incident detected?
    - When was the security incident first reported?
    - When was the security incident first detected?
    - What response activity has occurred to date?
    - What OpenText information may have or has been compromised?
        - Data potentially at risk? (PCI, PII, Proprietary)?
    - What is the current status of the incident?
    - Contact person we can reach out to (name, email, office number, cell number).

Business continuity and disaster recovery management

- Supplier must 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 the Supplier´s service.
- Supplier will regularly backup OpenText data and retain such OpenText backup data copies for a minimum of twelve (12) months.

About OpenText

OpenText enables the digital world, creating a better way for organizations to work with information, on-premises or in the cloud. For more information about OpenText (NASDAQ/TSX: OTEX), visit opentext.com.

Connect with us:

OpenText CEO Mark Barrenechea's blog

Twitter | LinkedIn