

THIRD PARTY SECURITY ANNEX (“TPSA”)

Whenever Supplier stores, processes, or otherwise accesses Confidential Information, or develops/provides products/software that is used by SAP or SAP customers, or otherwise has a material impact on SAP Systems, the Supplier must comply with all the requirements of this TPSA. The Supplier must also ensure that all of its Subcontractors (including any Subcontractor that is storing, using, or processing any Confidential Information in connection with Supplier’s delivery of Supplies to SAP) are contractually obliged to comply with the requirements of this TPSA.

1. Definitions.

- 1.1 “**Cardholder Data**” means: (i) with respect to a payment card, the account holder’s name, account number, security codes, card validation code/value, service codes (*i.e.*, the three or four digit number on the magnetic stripe that specifies acceptance requirements and limitations for a magnetic stripe read transaction), PIN or PIN block, valid to and from dates, and embedded data (including magnetic stripe data and EMV data); and (ii) information and data related to a payment card transaction that is identifiable with a specific account, regardless of whether or not a physical card is used in connection with such transaction.
- 1.2 “**Confidential Information**” means: all information, including Personal Data which SAP protects against unrestricted disclosure to others, furnished by SAP or its Representatives to Supplier or its Representatives (i) is identified as confidential, internal, or proprietary at the time of disclosure, or (ii) should reasonably be understood to be confidential at the time of disclosure given the nature of the information and the circumstances surrounding its disclosure.
- 1.3 “**Data Protection Law**” means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data in connection with the Services (and includes, as far as it concerns the obligations of Supplier and Subcontractors regarding the processing of Personal Data as described in applicable data processing agreements, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).
- 1.4 “**Data Subject**” means any individual or other person who is protected by Data Protection Law and whose data is processed by Supplier or a Subcontractor in connection with the Supplies.
- 1.5 “**Payment Card Industry Standards (“PCI Standards”)**” means: the security standards for the protection of payment card information with which the payment card companies collectively or individually require merchants to comply including, but not limited to the Payment Card Industry Data Security Standards currently in effect and as may be updated from time to time, and any other applicable payment card industry data security requirements for Cardholder Data that are currently prescribed by the PCI Security Standards Council and as may be updated from time to time during the term of the TPSA.
- 1.6 “**Personal Data**” means any information relating to a Data Subject which is protected under Data Protection Law, and in particular includes any information relating to an identified or identifiable natural or legal person; an identifiable person includes any person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity that is processed in relation to the Service.
- 1.7 “**Representatives**” mean: (i) Supplier Personnel; (ii) attorneys, accountants, or other professional business advisors; and, additionally, (iii) in the case of SAP, employees of SAP, SAP affiliates, customers, partners, and Subcontractors.
- 1.8 “**Security Incident**” means an unauthorized event that compromises the availability, integrity, or confidentiality of Confidential Information or Systems.
- 1.9 “**Supplier Personnel**” means: Supplier employees, as well as approved Subcontractors, agents, and/or other representatives that provide Supplies.
- 1.10 “**Supplies**” means: (i) services, including professional/consulting services (“Services”), (ii) physical items as well as software, data, scripts or code (“Goods”), and (iii) any Goods conceived, produced or developed in connection with the Services (“Deliverables”).
- 1.11 “**System**” means: a device or network of devices, virtual or actual, software, services and other elements that connect to store or process Confidential Information, including, without limitation, Supplies.

1.12“**Vulnerability**” means: a weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability.

2. Payment Card Industry (PCI) Compliance.

If Supplier collects, accesses, uses, stores, processes, disposes of or discloses Cardholder Data under this TPSA, Supplier shall at all times remain in compliance with PCI Standards, including remaining aware at all times of changes to PCI Standards and promptly implementing all procedures and practices as may be necessary to remain in compliance with PCI Standards, in each case, at Supplier’s sole cost and expense.

3. Security Management.

Supplier shall adopt, implement, maintain, update and monitor a written information security program that contains administrative, technical and physical safeguards designed to maintain service availability, data integrity, confidentiality and privacy of Confidential Information. This program shall include:

- 3.1 Executive review and support of all security related policies.
- 3.2 At least annual risk assessments of all assets relevant to SAP.
- 3.3 At least annual review of Security Incidents, including determination of root cause and corrective action.

4. Certifications/Attestations.

Supplier’s information security program shall be validated by applicable industry recognized external standards (e.g. ISO 27001, SOC 2, etc.). Supplier is required to submit to SAP all current and applicable certifications and attestations by using the electronic means as provided by SAP when available, and no more than annually. Supplier shall secure any rights necessary for SAP to share these certifications/attestations with SAP customers for whom the Supplier processes information or provides any type of indirect or direct maintenance or support. SAP is entitled to share such certifications or attestations with SAP customers upon request.

5. Security Incident.

- 5.1 Supplier shall maintain (internal or external) incident management and forensics capabilities, policies and procedures, including detailed security incident escalation procedures. In addition to the obligation to report a Personal Data Breach in the CDPA or MDPA (if applicable), Supplier shall notify SAP without undue delay at the SAP point of contact address <https://www.sap.com/about/trust-center/security/incident-management.html> whenever Supplier reasonably suspects that a Security Incident has occurred.
- 5.2 Supplier acknowledges that the SAP point of contact address covers multiple SAP affiliates, including SAP, and therefore agrees any such notices will contain a specific reference to “SAP Confidential Information.” In parallel with providing such notice, Supplier shall, without delay, investigate the Security Incident, take necessary steps to eliminate or contain the exposures that led to such Security Incident, and keep SAP advised of the status of such Security Incident and all matters related thereto. Upon SAP’s request, the Supplier must also provide an audit log of events that tracks System activity impacting Confidential Information.
- 5.3 Supplier further agrees to provide assistance, requested by SAP and/or SAP’s designated Representatives, in the furtherance of any investigation, correction and/or remediation of any such Security Incident, including any notification that SAP may determine appropriate to send to users, employees, customers or other individuals impacted or potentially impacted and/or the provision of credit monitoring services to such individuals, if credit monitoring services are required by applicable law.
- 5.4 To the extent permitted by applicable laws, Supplier shall not give notice to any regulatory authority, any individual or any Supplier of any actual or potential Security Incident without first consulting with and obtaining SAP’s written permission.
- 5.5 SAP reserves the right to (i) immediately suspend the receipt of any Supplies until it has determined that the Security Incident no longer poses a security or reputational risk to it, and (ii) conduct additional on-site security audits and reviews of information concerning Supplier’s security architecture, Systems and procedures, with full cooperation of the Supplier. In the event of a Security Incident directly resulting from Supplier’s failure to implement industry standard security measures, including standard encryption protocols and the requirements set forth

herein, Supplier shall bear all costs associated with required notifications and, if applicable, credit monitoring services as described above.

6. Human Resource Security.

Supplier shall take reasonable steps to ensure the reliability of all Supplier Personnel who have access to Confidential Information, including:

- 6.1 **Background Checks.** Supplier shall require all Supplier Personnel who will have access to Confidential Information to undergo and satisfy the requirements of a reasonable background investigation that Supplier conducts or causes to be conducted at its expense that is designed to confirm that none of such persons pose a threat to the safeguarding of Confidential Information or a threat to the integrity of the business operations of SAP or any of its customers. In executing its pre-hire screenings, Supplier is responsible for conducting its background checks and decisions in accordance with applicable laws.
- 6.2 **Adherence to Information Security Program.** Supplier shall require all Supplier Personnel to acknowledge in writing, at the time of hire and annually thereafter, to adhere to Supplier's Information Security Program and to protect all Confidential Information at all times, consistent with provisions of this Agreement. Such policy must be according to industry-accepted standards.
- 6.3 **Security and Privacy Awareness Training.** Supplier shall require all Supplier Personnel to undergo security and privacy awareness training at the time of hire and annually thereafter.
- 6.4 **Clean Desk Policy.** Supplier shall maintain a "clean desk" policy that ensures that whenever a user leaves its desk unattended during the day and prior to leaving the office at the end of the day, the user must ensure that documents containing Personal Data are placed in a safe and secure environment such as a locked desk drawer, filing cabinet, or other secured storage space.
- 6.5 **Disciplinary Policy and Process.** Supplier shall maintain a disciplinary policy and process, to be used when Supplier Personnel violate Supplier security policy or access Confidential Information without prior authorization.

7. Access Control.

Supplier shall use formal access management processes for the request, review, approval, and provisioning of all Supplier Personnel with access to any System. Access management controls will include:

- 7.1 Unique identifiers (user IDs) are required for access to all Confidential Information or Systems. Supplier shall ensure that procedures are in place so that requested user account creation, authorization changes, and access revocation are implemented promptly and only in accordance with approved policies and procedures that are based on industry best practices. Access to any data shall be restricted to Supplier Personnel and permissions shall be granted strictly on a "need-to-know" basis as needed for Supplier Personnel to fulfill their function.
- 7.2 In case Supplier Personnel leaves the company, their access rights must be revoked within 24 hours. When Supplier Personnel change their assigned role within the company, their access rights must be timely revoked or adapted. Supplier shall ensure that a password policy is implemented that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered.
- 7.3 Supplier shall utilize the principle of least access and shall not access, use, store, transfer, or disclose any Confidential Information, except as necessary to perform or deliver the Supplies.
- 7.4 Supplier shall implement a password policy that includes minimum requirements of length and complexity. All passwords must be changed if there is reasonable suspicion of a Security Incident. Passwords must be stored using industry accepted hashing algorithm; only administrators that support the function must have access to stored hashes, when necessary.
- 7.5 Supplier shall employ multi-factor authentication for all remote access to Systems.

8. Malware Control. Supplier shall maintain effective malware controls, including:

- 8.1 All Systems, all supporting Supplier Systems, and all laptop computers, desktop computers, and mobile devices that access Systems must be equipped with commercial-grade anti-virus, anti-malware, anti-spyware controls

that include real-time scanning, periodic whole-System scanning, and regular updates. These controls will also include signature or behavior-based detections of malware, viruses, spyware and trojans as it applies to ingress and egress points such as email services and file transfers and mitigation of security risks for malicious code on Systems, endpoints, and devices.

- 8.2 Supplier shall utilize spam-filtering Systems to block incoming messages containing spam and malware.
- 8.3 Supplier shall utilize web-filtering Systems to block access to Internet web sites containing or suspected to contain malware.

9. Data Encryption.

Data cannot be read or modified without authorization during transfer and at rest. Supplier shall use current commercial industry standard secure encryption methods to protect Confidential Information, including the following:

- 9.1 **Encryption of Transmitted Data.** Supplier shall use current industry standard secure encryption methods designed to encrypt communications during transit between its server(s) / service(s) and SAP browser(s) and between all its servers and all SAP's server(s) / service(s) / end-points. This applies to both physical and network-based data transfer. Data in transfer within secured networks and networks in control of Supplier must be appropriately secured.
- 9.2 **Encryption of Stored Data.** Supplier shall use industry standard secure encryption methods to encrypt data at rest, including on mobile devices such as laptop computers, designed to protect stored Confidential Information. Supplier shall store Confidential Information only on server(s) that are segregated from servers accessed from the Internet by other users of Supplier Supplies. Mobile devices that could provide access to devices or Systems where Confidential Information is stored must use Supplier controlled network encryption when connecting to Supplier networks remotely.
- 9.3 **Encryption Key Management.** Supplier shall have a defined key management policy that defines encryption key requirements, rotation, and lifecycle, including creation, distribution, revocation, archival, and destruction.

10. System Hardening.

Supplier shall use industry standard System and device hardening standards for all Systems that store, process, or transmit Confidential Information. Such hardening standards must include at minimum:

- 10.1 Disabling or removing all unnecessary services.
- 10.2 Security patch management implementations that provide regular and periodic deployment of relevant security updates.
- 10.3 Changing all default passwords.
- 10.4 Renaming administrative user accounts.

11. Business Continuity.

Supplier shall monitor and document the reliability, maintainability, serviceability and availability of Supplier's Systems or Supplies on a continuous basis. The Supplier shall maintain a Business Continuity Plan ("BCP") and conduct at least annual testing of the Supplier's BCP and provide a copy of the BCP and either the results or a report of the results of the test to SAP upon request.

12. Stipulation of Availability.

Supplier must ensure minimum availability of 99.99% per month, unless otherwise agreed upon in the relevant Statement of Work (SOW).

13. Vulnerability Management.

- 13.1 **Vulnerability Remediation.** Supplier shall implement a vulnerability management program that ensures that Vulnerabilities are remediated on a risk basis. Supplier shall install all Medium, High, and Critical security patches for all components in its production and development environment as soon as commercially possible.
- 13.2 **Vulnerability Notification.** Supplier shall notify SAP of a confirmed Vulnerability without undue delay by sending notice of it to: vas@sap.com. The notice must include (I) a description of the Vulnerability, (II) impacted products or Systems including the applicable versions, and (III) information reporting to the National Institute of Standards and Technology's Common Vulnerabilities and Exposures Program, including the CVE-ID, if applicable.

14. Data Management.

- 14.1 **Storage of Information.** Supplier shall store Confidential Information (to the extent permitted by the terms herein) only on assets authorized by Supplier's information security program. Data carriers shall be stored in secured areas.
- 14.2 **Authorized Equipment.** Supplier shall only use business equipment authorized in accordance with Supplier's information security program to perform or deliver the Supplies.
- 14.3 **Change of Supplier (Fourth Party) Subcontractors.** Supplier shall notify SAP at least 90 days in advance before changing Subcontractors that will have access to Confidential Information or System that transmit, store, or process Confidential Information. Supplier shall provide to SAP on request any due diligence that was conducted to determine the Subcontractor's suitability for performing or delivering Supplies supporting SAP or SAP customers. If applicable, Supplier shall also provide information as reasonably requested by SAP about the security practices and procedures of the selected provider, including its physical security controls and environment. SAP reserves the right of termination, both for Supplier's breach of security practice standards or for violation of the 90-day limit.
- 14.4 **Change of Supplier Processes.** Supplier shall provide SAP of written notice of any material changes to processes used to support SAP or SAP customers at least 30 days prior to implementing such changes.
- 14.5 **Return/Destruction of Data.** As between SAP and Supplier, all Confidential Information and data carriers and any copies, reproductions, summaries, analyses or extracts thereof or based thereon, including (without limitation) those created by Supplier in connection with the performance or delivery of the Supplies, shall remain the property of SAP (including all customer and Supplier data for which SAP is responsible). Supplier shall promptly return such Confidential Information and data carriers to SAP via SAP approved methods upon the earliest of the following events: (i) SAP's request; or (ii) completion of Supplies; or (iii) expiry or termination of any agreement under which Supplies are delivered. Alternatively, where Confidential Information and/or data carriers cannot be returned, or if SAP elects so, Supplier shall permanently destroy all Confidential Information in its possession or control and data carriers which otherwise would have to be returned in accordance with this Section 14.5. Supplier shall provide SAP with a written certificate of destruction. The written certificate of destruction shall detail the destruction method used to permanently destroy all Confidential Information and/or data carriers, the date of destruction and individual who performed the destruction. Supplier's destruction of Confidential Information under this Section shall comply with industry standard practices.

15. Secure Development.

- 15.1 Supplier ensures that all Systems developed by the Supplier to provision Supplies are developed following a secure software development lifecycle process which includes industry best practices for achieving and sustaining required security qualities for confidentiality, integrity and availability protection. Supplier shall ensure that software security vulnerabilities (see, for example the OWASP Top Ten or CWE listings) are addressed via Supplier's vulnerability management program prior to deployment.
- 15.2 Supplier shall implement and maintain security measures and controls for Supplies relating to software provisioning that are adequate to meet business, technology and regulatory risks according to international standards such as ISO/IEC 27034. Such security measures and controls will include at minimum: security education of the development workforce, secure architecture and design principles, secure coding practices, security testing methods and tools applied, security response to react timely on applicable software vulnerabilities that become known, as well as application security controls embedded and enforced by the software itself, such as identity management, authentication, authorization, encryption etc.

15.3 Supplier shall have procedures in place to ensure integrity of software updates which will ensure that the Supplies or open-source software used for providing the Supplies do not contain known backdoors, viruses, trojans or other kind of malicious code.

16. Security Audits by SAP.

16.1 SAP is entitled to carry out annual security audits on the Systems, security processes and procedures of the Supplier and any time upon prior notification in the case of a request from an external authority, reasonable suspicion of a Security Incident or findings in documented security audits or other documentation provided to SAP.

16.2 Should SAP require a security scan of Supplier's resources containing Confidential Information to identify or validate deficiencies, SAP shall identify the tools used for testing and the methods used. SAP and the Supplier shall mutually agree to the scope, approach and timing of such testing so that scanning does not interfere with Supplier's normal business operations and performance.

16.3 Audit results shall contain only relevant information for the Supplies provided to SAP. If security vulnerabilities are discovered during the check, the Supplier shall promptly take reasonable steps to mitigate the security vulnerabilities and to minimize any potential risk.

17. NDAA 889 Requirement.

Compliance with the 2019 National Defense Authorization Act Section 889. If applicable, the Supplier warrants and certifies that in providing the Supplies and in the performance of this agreement, it shall not supply SAP with, or utilize in the performance of the Supplies, any (a) "covered telecommunications equipment or services" as more specifically described in the United States Federal Acquisition Regulation clause 52.204-25, "Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment or (b) goods or services produced or supplied by entities identified as Chinese Military Companies pursuant to Section 1260H of the 2021 National Defense Authorization Act or (c) Covered Telecommunications Equipment or Services as specified in section 2(a) of the Secure and Trusted Communications Networks Act of 2019, available at: www.fcc.gov/supplychain/coveredlist

18. Regulatory and Legal requirements.

Under the applicable regulations and laws, SAP and its customers are required to execute enhanced audit, disaster recovery (including backups) and other data protection requirements, current or in the future, whether directly or in support of customer's obligations. Accordingly, Supplier shall:

18.1 Allow SAP, its customers, and regulators on-site and remote audit rights to the extent required by law.

18.2 Provide responses to questionnaires to the extent specific responses are required by applicable regulations and laws.

18.3 Ensure reasonable cooperation and confidentiality during audits and such actions.

19. SAP Third Party Risk Management (TPRM).

Supplier shall undergo and complete the SAP TPRM assessment process by responding fully and accurately to applicable questionnaires and providing corresponding evidence and documentation as needed. Upon the conclusion of the TPRM assessment process, Supplier shall collaborate with SAP to remediate any findings identified during the process within mutually agreed timelines. Supplier shall undergo and complete the SAP TPRM reassessment process at least once every twelve (12) months following the conclusion of any prior SAP TPRM assessment or reassessments.

20. Data Protection Officer.

If Supplier is processing Personal Data on behalf of SAP, Supplier shall designate a data protection officer (or a responsible person if a data protection officer is not required by law).

21. Additional Requirements for Supplier IT Infrastructure.

If Supplier has been identified as a Supplier that delivers Supplies (including, if applicable, the processing and storage of Personal Data) in the Systems/infrastructure of the Supplier or its Subcontractors, the following additional terms will apply:

21.1 Data Center Certifications/Attestations.

For all data center services, Supplier must be certified against ISO 27001 and provide SOC2 Type 2 reports as a minimum, and if applicable, must be certified against PCI and provide SOC 1 type 2 reports. If data center services are subcontracted by the Supplier, the Supplier must ensure their Subcontractors are also in compliance with these minimum requirements.

21.2 Penetration Testing.

Supplier shall provide to SAP summary results of penetration testing undertaken by the Supplier of any Supplies processing Confidential Information, upon request at Supplier's expense. Such testing shall occur at least once every twelve (12) months. If any such reports include any findings flagged as "critical" or "high" security risks (industry standards like Common Vulnerability Scoring System should be used for vulnerability rating), Supplier shall promptly remediate such findings, and either provide written confirmation of their remediation or conduct additional penetration tests and submit a new report to SAP as evidence of the findings' remediation. SAP is entitled to share these reports with SAP customers for whom the Supplier processes information or provides any type of indirect or direct maintenance or support.

21.3 Physical Access Control.

Supplier shall ensure its formal access management process includes controls such as:

21.3.1 Multiple authorization levels are used when granting access to sensitive Systems, including those storing and processing Personal Data. Authorizations must be managed via defined processes ensuring access to data centers or rooms where data servers are located are appropriately restricted. Supplier Personnel without access authorization (e.g. technicians, cleaning personnel) must be accompanied at all times.

21.3.2 For data centers, video surveillance and alarm devices must be used with reference to access areas.

21.4 Network Security.

Supplier must ensure the following network security controls are in place in Supplier's Systems:

21.4.1 Supplier shall maintain network-based intrusion detection/intrusion prevention system(s) to detect and prevent unwanted or hostile network traffic. Upon the availability of updates, Supplier shall update its intrusion detection/prevention software promptly and without delay.

21.4.2 Supplier shall utilize commercial-grade firewalls that restrict all inbound and outbound traffic except for those specific ports and IP addresses necessary to deliver the Supplies.

21.4.3 Supplier shall ensure that Denial-of-Service (DoS) preventive measures are in place for any applicable data center involved with providing the Supplies.

21.5 Vulnerability Management

21.5.1 **Infrastructure Scans.** Supplier shall perform periodic vulnerability scans at least once a month on all infrastructure components of its production and development environment. Supplier shall ensure that all applicable Supplier Subcontractors perform periodic vulnerability scans at least once a month on all infrastructure components of the Subcontractor's production and development environment.

21.5.2 **Application Scans.** Supplier shall perform security code reviews, including both static testing and dynamic testing, promptly, whenever changes occur to source code, or when new code is deployed.

21.6 Data Management

21.6.1 **Segregation of Data.** Supplier shall use physical and/or logical controls to segregate Confidential Information from that of other Supplier customers. Supplier shall produce documentation describing data segregation controls to SAP upon request.

21.6.2 **Backups.** Supplier shall make backup copies of information, software and System images shall be taken and tested regularly. Backups shall be stored in specially protected environments.

21.7 Security Logs.

Supplier shall employ procedures that all Systems, including firewalls, routers, network switches and operating Systems, log information to their respective System log facility or a centralized logging System to enable the security audits described in this agreement. Supplier shall continuously and actively detect Systems and infrastructure against attacks and for risk and functional anomalies through operation of an enterprise threat detection System and additional tools, including using and analyzing logs. Additionally, Supplier shall employ the following procedures:

21.7.1 Logs shall be retained for at least one (1) year.

21.7.2 Logs shall be protected from unauthorized modification or erasure.