THIRD PARTY SUPPLIER 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 can otherwise materially impact SAP systems, supplier shall comply with the requirements of this TPSA and shall contractually require all of its sub-processors (including any subcontractor that is storing, using, or processing any Confidential Information in connection with Supplier's delivery of Supplies to SAP) to comply with the requirements of this TPSA.

1. Definitions.

   a. "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.

   b. "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.

   c. "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.

   d. "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. PCI Compliance. If Supplier has access to or will collect, access, use, store, process, dispose of or disclose Cardholder Data under this TPSA, Supplier shall at all times remain in compliance with the PCI Standards, including remaining aware at all times of changes to the PCI Standards and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI Standards, in each case, at Supplier's sole cost and expense.

3. Security Management. Supplier shall adopt, implement, maintain 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, which program shall include:

   a. Executive review and support of all security related policies.
   b. Periodic (but no less than annual) risk assessments of all assets relevant to SAP.
   c. Periodic review of security incidents, including determination of root cause and corrective action.
   d. Periodic internal audit to measure the effectiveness of controls.

4. Security Standards. Supplier shall adhere to at least one of the following industry recognized security standards: ISO/IEC 27001 – Information Security Management Systems, or ISO-IEC 27002 – Code of Practice for International Security Management, the COBIT standards, NIST, or the PCI Standards.

5. Certifications/Attestations. Supplier is required to submit to SAP all current and applicable ISO/BS certifications (e.g., ISO27001 and ISO22301), System Organizational Control Reports (e.g., SOC2) or other certifications and attestations when available, and no more than annually, depending on the frequency of such audits, by using the electronic means as provided by SAP. Third Party 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.

6. Data Center Certifications/Attestations. Supplier must be certified against ISO 27001, PCI and provide SOC1 and SOC2 Type 2 reports as a minimum for all data center services. If data center services are subcontracted by the Supplier, the Supplier must ensure their subcontractors are also in compliance with these minimum requirements.

7. Penetration Testing. Supplier shall provide to SAP summary results of penetration testing undertaken by the Supplier of any Service processing Confidential Information, upon request at Supplier's expense. Such testing shall occur no less frequently than once every twelve (12) months. If any such reports include any findings flagged as "critical," "high" or "medium" security risks (industry standards like Common Vulnerability Scoring System should be used for vulnerability rating), Supplier shall promptly fix such issues, undergo additional penetration testing, and provide a new report to SAP without any issues flagged as such level security risks. 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.

8. Security Incident. 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 (if applicable), Supplier shall notify SAP immediately (which in no event will be longer than twenty-four (24) hours) at https://www.sap.com/about/trust-center/security/incident-management.html whenever Supplier reasonably suspects that any Confidential Information or Systems have been accessed, acquired, used or disclosed by any unauthorized person, or by any person in an unauthorized manner or for an unauthorized purpose ("Incident"). Supplier acknowledges that this SAP point of contact address covers multiple affiliates, including SAP, and therefore agrees any such notices will contain a specific reference to "SAP Data." In parallel with providing such notice, Supplier shall without delay investigate the Incident, take necessary steps to eliminate or contain the exposures that led to such Incident, and keep SAP advised of the status of such Incident and all matters related thereto. Upon SAP's request, the Supplier must also provide an audit log of events that tracks service activity impacting Confidential Information upon SAP's request. 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 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 service to such individuals, if and to the extent credit monitoring is required by applicable law. To the extent permitted by applicable laws or regulations, Supplier shall not give notice to any regulatory authority, any individual or any Supplier of any actual or potential Incident without first consulting with and obtaining SAP's written permission. SAP reserves the right to (i) immediately suspend any Services until it has determined that the Incident no longer poses a security or reputational risk to it, and (ii) immediately conduct additional on-site security audits and reviews of information concerning Supplier's security architecture, Systems and procedures. In the event of an Incident directly resulting from Supplier's failure to use industry standard security measures, including standard encryption protocols and the requirements set forth herein, Supplier shall be responsible for the cost of notification and, if applicable, credit monitoring as described above in this paragraph.

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

   a. 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 other 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. At a minimum (and at all times in accordance with applicable laws which may impose greater or different requirements), in order to be reasonable hereunder, background checks must include the following:

      For Supplier Personnel in the United States:
      - SSN Trace
      - 7 Year County Criminal Report
      - 7 Year Statewide Criminal Report
      - 7 Year Federal Criminal Report
      - Basic Employment Verifications (all employment within 7 years)
      - Education Verification (highest degree earned)
      - Multi-state / Multi Jurisdiction Criminal Search
      - Status on the Office of Foreign Assets Control (OFAC) list

      For Supplier Personnel outside the United States:
      - SSN or (or SSN equivalent) Trace (inapplicable if jurisdiction does not have an SSN equivalent)
      - International Criminal Search (checking all locations listed on candidate profile)
      - International Employment Verifications (checking all employment within past seven years)
      - Education Verification (checking highest degree earned)

   b. Adherence to Security Policy. Supplier shall require all Supplier Personnel to acknowledge in writing, at the time of hire and annually thereafter, to adhere to Supplier's security policy and to protect all Confidential Information at all times, consistent with provisions of this Exhibit. Such policy must be according to industry-accepted standards.
   c. 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.
   d. 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.

10. Access Management. 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:

    a. Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes.
    b. Unique identifiers (user IDs) are required for access to all Confidential Information or Systems. Procedures are in place so that requested user accounts and authorization changes are implemented only in accordance with approved policies and procedures that are based on industry best practices (for example, no rights are granted without authorization).
    c. In case Supplier Personnel leaves the company, their access rights are revoked within 24 hours. When Supplier Personnel change their assigned role within the company, their access rights are

timely revoked or adapted. Supplier has a password policy 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. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, Systems force a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver

d. Display screens for all systems that could disclose information allowing access to another Supplier's device or system or screens used to handle Confidential Information should be positioned so that unauthorized persons cannot readily view them through a window, over a shoulder, or by similar means.

e. Mobile devices that could provide access to devices or systems where Confidential Information is stored must be kept in the possession of Supplier Personnel or locked in a secure location when not in use. Mobile devices must not be checked in as luggage when travelling.

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

    a. All Systems, all supporting Supplier systems, and all laptop computers, desktop computers, and mobile devices that access Systems will include commercial-grade anti-virus, anti-malware, anti-spyware controls that include real-time scanning, periodic whole-system scanning, and regular updates. This includes 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. It also mitigates security risks for malicious code on systems, endpoints, and devices.
    b. Supplier shall utilize spam-filtering systems to block incoming messages containing spam and malware.
    c. Supplier shall utilize web-filtering systems to block access to Internet web sites containing or suspected to contain malware.
    d. Supplier shall utilize commercial-grade firewalls that restrict all inbound and outbound traffic except for those specific ports and IP addresses necessary to perform the Service. Supplier continuously and actively detects systems and infrastructure against attacks through operation of an enterprise threat detection system and additional tools, including using and analyzing audit logs.

12. Intrusion Detection/ Intrusion Prevention. 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 by the software provider, Supplier shall update its intrusion detection/prevention software promptly and without delay.

13. 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:

    a. Encryption of Transmitted Data. Supplier shall use current Internet-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 is appropriately secured.
    b. Encryption of Stored Data. Supplier shall use Internet-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 use Supplier controlled network encryption when connecting to Supplier networks remotely.

c. 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.

14. System Hardening. Supplier shall use Internet-industry standard system and device hardening standards for all Systems that store, process, or transmit Confidential Information. Such hardening standards will include:

    a. Disable or remove all unnecessary services.
    b. Security patch management is implemented to provide regular and periodic deployment of relevant security updates.
    c. Change all default passwords.
    d. Rename administrative user accounts.
    e. Each server performs only one function (e.g., web server, application server, and database server should occupy separate systems).
    f. Employ host-based intrusion detection and prevention mechanism.
    g. Passwords are stored using industry accepted hashing algorithm; only administrators that support the function have access to stored hashes, when necessary.

15. Business Continuity. Supplier will ensure to monitor and document the reliability, maintainability, serviceability and availability of a system or service on a continuous basis. The Supplier shall conduct at least annual testing of the Supplier's Business Continuity Plan and provide a copy of the Business Continuity Plan and the results of the test to SAP upon request.

16. Stipulation of Availability. Supplier should ensure minimum availability of 99.99% per month, unless otherwise agreed upon in the relevant Statement of Work (SOW). Supplier will ensure Denial-of-Service (DoS) preventive measures are in place for the data center providing the service.

17. Vulnerability Management.

    a. Infrastructure Scans. Supplier shall perform periodic (but no less than once per month) vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities shall be 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.
    b. Application Scans. Supplier shall perform periodic (but no less than once per quarter, as well as after making any change to the Supplier System application vulnerability scans). Vulnerabilities shall be 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.
    c. External Application Testing. Supplier shall perform security code reviews, including both static testing and dynamic testing whenever changes occur to source code, or when new code is deployed.
    d. 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.

18. Data Management.

a. Storage of Information. Supplier shall store Confidential Information (to the extent permitted by the terms herein) only on servers controlled by Supplier and/or its third-party hosting provider. End user workstations, laptops, USB devices, CD-ROM, DVD-ROM, and mobile devices shall not be used to store any Confidential Information.

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

c. Backups. Supplier shall protect Confidential Information against loss, backup copies of information, software and system images shall be taken and tested regularly.

d. Change of the Hosting Provider. Supplier shall notify SAP at least 90 days in advance before changing or adding a hosting provider for Data or System deployment and such notice will identify the selected hosting provider (or provider options under consideration by Supplier). Supplier shall provide information as reasonably requested by SAP about the security practices and procedures of the selected provider, including its physical security controls and environment. In the event SAP reasonably determines that the security practices and physical security of the new provider are not sufficient or comparable to those employed by the hosting provider previously used by Supplier, SAP may terminate an Order with written notice of at least fifteen (15) days.

e. 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. SAP reserves the right of termination, both for Supplier's breach of security practice standards, or for violation of the 90-day limit.

f. Change of Supplier Processes. Supplier shall notify SAP of any major changes to processes the Supplier uses to support SAP or SAP customers at least 30 days in advance.

g. 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 made by Supplier in performance or delivery of the Supplies, are the property of SAP (including all customer and Supplier data SAP is responsible for) and shall be promptly returned via SAP approved methods to SAP upon any of the following events, whichever is earliest: (i) upon SAP's request; or (ii) upon completion of Supplies; or (iii) upon 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 destroy and certify to SAP in writing that it has permanently destroyed all Confidential Information in its possession or control and data carriers which otherwise would have to be returned in accordance with this Section 16(d). 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 be in compliance with industry standard practices.

h. Supplier shall not access, use, store, transfer, or disclose any Confidential Information, except as necessary to perform or deliver the Supplies.

19. 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 in order to enable the security audits referred to below. Additionally, Supplier shall employ the following procedures:

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

    b. Logs shall not contain Confidential Information.

    c. Logs shall be protected from unauthorized modification or erasure.

d. Logs shall be backed up on a daily basis.
e. Logs shall be monitored for risk and functional anomalies.

20. Secure Remote Access. Supplier shall employ two-factor authentication for all remote access to internal and confidential information and systems.

21. Data Retention. Data will be securely retained for the time requirements and in the manner in accordance with privacy and regulatory laws for the region of demographic persons that the Supplier creates, stores, or processes. This may continue after the primary engagement or project is closed.

22. Issue Remediation Supplier agrees to work with SAP and their designees to remediate issues or risks identified through assessments, conducted on behalf of SAP or conducted on behalf of the Supplier. Supplier shall remediate at its cost those issues identified as high within 30 days, those identified as Medium or low within 90 days, provided that an issue is within the reasonable control of the Supplier.

23. Secure Development. Supplier ensures that all Supplies developed by for the Supplier to provision Supplies have been 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. In addition, software security vulnerabilities (see, for example the OWASP Top Ten or CWE listings) shall be avoided. The expected security measures and controls applied for software provisioning, such as 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. shall be adequate to meet relevant business, technology and regulatory risks according to international standards such as ISO/IEC 27034. The Supplier has procedures in place to ensure integrity of software updates and can demonstrate that precautions are taken to ensure that any own or Supplier or open source software used for providing the Supplier Supplies do not contain known backdoors, viruses, trojans or other kind of malicious code.

24. Security Audits by SAP. SAP is entitled to carry out security audits on the systems, security processes and procedures of the Supplier at least once per year 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. Should a security scan of Supplier's resources containing Confidential Information be required 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. Audit results shall contain only relevant information for the Supplies provided to SAP. If security vulnerabilities are discovered during the check, the Supplier shall take reasonable steps to mitigate the security vulnerabilities and to minimize any damage from the security incident.

25. NDAA 889 Requirement. Compliance with the 2019 National Defense Authorization Act Section 889. If applicable, the Supplier does not utilize equipment or Supplies provided by Huawei, ZTE, Hytera, Hikvision, or Dahua or their subsidiaries.

26. 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 will:

a. Allow regulator or customer on-site audit rights to the extent required by law.
b. Provide responses to questionnaires to the extent specific responses are required by applicable regulations and laws.
c. Allow for customer termination rights for any deficiencies or noncompliance with this agreement or any applicable regulation or laws that requires such right under the applicable circumstances.

27. SAP Supplier Risk Management (TPRM) Process. Supplier is required to undergo and complete the SAP TPRM process. In addition, Section “Issue Remediation” will apply for issue remediation. SAP reserves the right of service termination in both cases, if either the SAP TPRM Process or the issue remediation is not completed.