SAP SUPPLIER SECURITY STANDARD TERMS

1. APPLICABILITY

These Supplemental Terms to the SAP Procurement General Terms and Conditions as posted on the SAP Supplier Portal only apply to Suppliers who may access and/ or process SAP or SAP Customer confidential information, e.g. by providing customer facing, SAP cloud related services. Reporting of Security Incidents

The Supplier is required to inform SAP promptly of all critical security incidents without undue delay to the designated SAP point of contact: https://www.sap.com/about/trust-center/security/incident-management.html.

A security incident is defined as unwanted or unexpected information security events that have a significant probability of compromising SAP business operations and threating SAP information security.

2. SECURITY AUDITS BY THE SUPPLIER

The Supplier shall be obliged to verify that the releases of its IT systems, applications and services documented in the configuration or release database are correct and to inspect its systems for security vulnerabilities, by performing annual penetration tests on its own systems. These records are to be kept in a retrievable form and made available in the case that a security audit is performed by SAP.

3. CERTIFICATIONS/ATTESTATIONS

The Supplier is required to submit all current and applicable ISO/BS certifications (e.g. ISO27001 and ISO22301), Service Organizational Control Reports (e.g. SOC2) or other certifications and attestations on an annual basis by using the electronic means as provided by SAP.

4. SECURITY VALIDATION BY SAP

SAP is entitled to carry out non-invasive security validation on the systems of the Supplier at 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. For this purpose, the confidentiality terms in the SAP Procurement General Terms and Conditions apply also to confidential information of Supplier. 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 services 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.

5. DATA CENTERS AS SUBCONTRACTORS

The Supplier must be certified against ISO 27001 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 ISO 27001 certified as a minimum requirement. In addition, section 3 will apply.

6. SECURITY PRINCIPLES

The Supplier agrees to fulfill the following security principles as stipulated in this section:

6.1. Data in transit protection

The Supplier will adequately protect SAP and SAP customer data transiting networks against tampering and eavesdropping using a combination of network protection and encryption. No unprotected HTTP connections are allowed. TLS, the protocol underlying secure HTTPS connections, must be configured on the connecting server with a minimum of: minimum TLSv1.2 with forward secrecy, no known insecure cryptographic primitives like SHA-1 or RC4, minimum key size of 2048bits of RSA and 256bit for EC. Any other used protocols used must be secured and encrypted.

6.2. Asset protection and resilience

The Supplier will protect SAP and SAP customer data, and the assets storing or processing it, against physical tampering, loss, damage or seizure. Controls will exist on the following: Physical location and legal jurisdiction; data center security or security of location of data; data at rest protection (physical access to data); data sanitization (off-boarding process); equipment disposal; physical resilience and availability (IT disaster recovers/business continuity).

6.3. Separation of data

The Supplier will ensure that separation exists between different data involved in a service to prevent malicious or compromised users from affecting the service or data of another service.

6.4. Governance

The Supplier will govern security to coordinate and direct their overall approach to the management of the service and information within: Industry standard security policies and security standards; defined responsibilities and risk based decision-making authority processes.

6.5. Operational Security

The Supplier will have processes and procedures in place to ensure the operational security of the service provided including: configuration and change management; security patch management; vulnerability management; protective monitoring; security incident management; secure decommissioning.

6.6. Personnel Security

The Supplier will ensure that personnel security screening and/or security education is performed regularly and is adequate for all resources utilized to provide the contracted services to SAP.

6.7. Secure Development

The Supplier ensures that all software and services used by the Supplier to provision the Supplier services, including those developed by the Supplier and those provided by others, have been developed following a 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 3rd party or open source software used for providing the Supplier services do not contain known backdoors, viruses, trojans or other kind of malicious code.

The Supplier will ensure that SAP is provided with the tools required to help SAP securely manage the service.

6.8. Identity and authentication

The Supplier will ensure that access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorized individuals. Integration with SAP ID Service (SAMLv2) is required.

6.9. External interface protection

The Supplier will ensure that all external or less trusted interfaces of the service are identified and have appropriate state of the art protections to defend against attacks through them.

6.10. Secure service administration

The Supplier will ensure that the methods used by administrators to manage the operational service are designed to mitigate any risk of exploitation that could undermine the security of the service. Remote administration sessions must be encrypted, use at least two-factor for authentication, access to the systems administered must be restricted by IP addresses used by the Supplier by means of access control lists, all access must be logged.

6.11. Availability Management

The Supplier will ensure to monitor and document the reliability, maintainability, serviceability and availability of a system or service on a continuous basis.

Supplier agrees all products or services licensed to SAP, other than beta-stage products which are on their face clearly not subject to the same terms and conditions as final released products, will be accompanied by a Service Level Agreement identifying a minimum availability percentage (SLA); Vendor furthermore agrees that if such SLA does not exist, it will ensure minimum availability of 99.99% per month.

7. RIGHTS TO INFORMATION AND EXAMINATION

The Supplier will ensure that SAP has the rights to information and examination for the relevant supervisory authorities, SAP, its internal auditing department and its auditors of financial statements (Examiners).