# SAP FIONEER SUPPLIER SECURITY STANDARD ANNEX

The Supplier hereby agrees as follows:

## 1. SCOPE AND GENERAL CONDITIONS

This Supplier Security Standard Agreement mandates the requirements of the Supplier to provide services to SAP Fioneer, SAP Fioneer GmbH, and /or SAP Fioneer Affiliates under the Agreement.

## 2. COMMUNICATION CHANNEL

2.1 The Supplier shall contact and inform SAP Fioneer at security@SAP Fioneer.com or mutual agreed channel for any specific case.

2.2 SAP Fioneer will contact the Supplier at [add Supplier email contact] or mutual agreed channel for any specific case.

## 3. REPORTING OF SECURITY INCIDENTS

A security incident is an unwanted or unexpected information security events that have a significant probability of compromising SAP Fioneer business operations and threating SAP Fioneer information security including confidentiality, integrity or availability of services and data.

The Supplier is required to inform SAP Fioneer without undue delay of all critical security incidents to the designated SAP Fioneer point of contact.

## 4. INFORMATION ABOUT DEVELOPMENTS

The Supplier conducts regular internal monitoring and will issue reports about this to SAP Fioneer at least every 6 months. The Supplier will inform SAP Fioneer without undue delay about internal or external developments which could have an adverse effect on the proper performance of the further outsourced activities and processes.

## 5. 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 Fioneer.

## 6. CERTIFICATIONS/ATTESTATIONS

Regardless of the reports which have to be provided in accordance with the service description the Supplier is required to submit all current and applicable ISO/EN/BS certifications (e.g. ISO27001 and ISO22301, BS10012), Service Organizational Control Reports (e.g. SOC2, C5) or other certifications and attestations relevant for the provided Services on an annual basis by using the electronic means as provided by SAP Fioneer.

In addition, the Supplier will report regularly, but at least quarterly, possible impairments of performance on the provided services, and its solutions to SAP Fioneer. The Supplier grants SAP Fioneer the right to share such Certifications and reports with the End User of SAP Fioneer.

## 7. SOFTWARE SUPPORT AND MAINTENANCE SERVICES

The Supplier must be certified against ISO 27001 and ISO9001 as a minimum for all software development, maintenance, and support services. If Software maintenance and support services are subcontracted by the Supplier, the Supplier must ensure their subcontractors are also certified and audited on the same standards as a minimum requirement.

## 8. CLOUD AND DATA CENTERS SERVICES

The Supplier must be certified against ISO 27001 an audited against AT101/ISAE3000-SOC2 type II as a minimum for all cloud services and data center services. If cloud services or data center services are subcontracted by the Supplier, the Supplier must ensure their subcontractors are also certified and audited on the same standards as a minimum requirement.

**9. RIGHTS TO INFORMATION AND EXAMINATION**

9.1 The Supplier will ensure that SAP Fioneer has the unrestricted rights to information, inspection and examination for SAP Fioneer, the relevant supervisory authorities having jurisdiction over SAP Fioneer and/or SAP Fioneer's End Users, and where required by applicable law or regulation End Users of SAP Fioneer, their internal auditing departments, their auditors of financial statements and any third party auditor engaged for the purpose ("Examiners").

9.2 The Examiners can examine compliance with the provision of supervisory law at the Supplier as well as the individual requirements of the individual supervisory authorities regarding the services for which SAP Fioneer has issued the contract. The Examiners have a comprehensive and unhindered right to inspect and examine at any time which includes preparing copies of relevant records. The Examiners especially receive access to all documents, data media and systems, locations at the Supplier to the extent they relate to these services for which SAP Fioneer has issued the contract. The Supplier grants the Examiners a right of entry to its business premises for the purpose of exercising the right to information and the right to examine. Persons exercising internal audit functions at the Supplier or engaged in external audits required by law or ordered under supervisory law must be released from their duty to remain confidentiality towards Examiners.

9.3 The examination rights exist after the end of the services for which SAP Fioneer has issued the contract for a period of at least five (5) years, beginning at the end of the SAP Fioneer customer's financial year in which all services under this SSSA have ended; relevant records must remain available for just as long, without regard to any other statutory retention periods, unless the Supplier has surrendered these records to SAP Fioneer or the customer of SAP Fioneer when the contract ends as agreed in the contract.

9.4 SAP Fioneer and as required by applicable law or regulations SAP Fioneer's End Users are entitled to carry out non-invasive security validation on the systems of the Supplier at any time upon prior notification. During the security validation, among other checks, security scans are carried out. To this end, automated and manual tests are simulated on the software, networks, or systems involved. 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.

9.5 Each Party bears its own costs incurred under this Clause 9.

**10. AUTHORITY OF SAP FIONEER TO ISSUE DIRECTIVES**

10.1. SAP Fioneer can issue directives to the Supplier regarding the services for which SAP Fioneer has issued the contract. SAP Fioneer can especially pass on to the Supplier orders and directives of the relevant supervisory authorities issued to the End User of SAP Fioneer in the form of directives or to the extend required by applicable law or regulation directives issues by the End User of SAP Fioneer

10.2. Directives should be issued in text form. The Supplier will confirm to SAP Fioneer the directive in writing upon request.

10.3. If SAP Fioneer issues an oral directive in a specific case, SAP Fioneer must confirm the directive in text form without undue delay.

10.4. If adjustments to the services for which SAP Fioneer has issued the contract or the type and manner of performance of the services become necessary due to directives, the Supplier can demand compensation in accordance with the provision on compensation in this SSSA. The Supplier must implement the directive in a cost-efficient manner.

**11. USE OF THIRD PARTIES**

The Supplier can involve third parties in the performance of the services for which SAP Fioneer has issued the contract only after prior written consent of SAP Fioneer; this reservation for consent also extends to the scope and modalities of the services as well as the content of the contract with the third party. The Supplier will conclude contractual agreements which are consistent with the provisions in this SSSA. The contract with the third party will especially provide that rights of information, inspection and examination existing under Clause 9 of this Annex can be exercised directly against the third party. The Supplier will submit to SAP Fioneer the contract with the third party upon request. The Supplier can redact the commercial agreements with the third party prior to handing the contract over to SAP Fioneer. SAP Fioneer can disclose the contract with the third party to SAP Fioneer's customer.

## 12. SECURITY PRINCIPLES

The Supplier agrees to fulfill the following security principles as relevant for the provision of the Service provided to SAP Fioneer:

### 12.1 Encryption of Data

The Supplier will adequately protect SAP Fioneer and SAP Fioneer' End User's data transiting networks against tampering and eavesdropping using a combination of network protection and encryption. No unprotected connections are allowed. HTTPS connections must be configured on the connecting server with a minimum of minimum TLSv1.2 with forward secrecy, and blocking of 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 on a similar security level.

The Supply will encrypt digital data at rest with current Industry Standard methods.

### 12.2 Asset protection and resilience

The Supplier will protect SAP Fioneer and SAP Fioneer's End User 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).

### 12.3 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.

### 12.4 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.

### 12.5 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.

### 12.6 Personnel Security

The Supplier will ensure that adequate regular personnel security screening and adequate at least yearly security education is performed for all resources utilized to provide the contracted services to SAP Fioneer.

### 12.7 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 good practices 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.

## 13. SECURE MANAGEMENT

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

13.1 **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 Fioneer ID Service (SAMLv2) is required.

13.2 **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.

13.3 **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.

13.4 **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. The Supplier should ensure minimum availability of 99.99% per month, unless otherwise agreed upon in the relevant Agreement.