Technical and Organizational Measures (TOMs) for SAP Fioneer Services

This document describes the Technical and Organizational Measures that apply to the production instance of Cloud Services, SAP Fioneer Support provided by SAP Fioneer or its Subprocessors and Consulting Services conducted from SAP Fioneer premisses and systems (jontly "SAP Fioneer Services"). SAP Fioneer may change these Technical and Organizational Measures at any time without notice so long as it maintains an equivalent or better level of security.

1. PHYSICAL ACCESS CONTROLS

Only authorized persons can physically access premises, buildings or rooms where Data is stored. SAP Fioneer protects its assets and facilities using the following means:

1.1 Data centers and infrastructure systems are designed to minimize the impact of environmental risks including damage caused by natural disasters.

1.2 As a minimum requirement, the physical entrance points of the office buildings and the data center facilities are fitted with a key system.

1.3 Depending on the security classification, buildings, specific areas and surrounding premises are further protected by additional security measures. These include specific access profiles, video surveillance, intruder alarm systems, smart card access control, active key management and biometric access control systems.

1.4 Access rights are granted to authorized persons on an individual basis according to the System Access Control and Data Access Control measures. This also applies to visitor access. Guests and visitors to SAP Fioneer buildings have to register at the reception and will be accompanied by authorized SAP Fioneer personnel.

1.5 Only authorized persons have access to systems and infrastructure within the data center facilities.

1.6 Every person has to wear their ID cards at all SAP Fioneer locations.

1.7 Additional measures for SAP Fioneer operated data centers:

(a) All data centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and data center facilities from being compromised. To protect proper functionality, physical security equipment (e.g. motion sensors, cameras) undergo regular maintenance.

(b) SAP Fioneer logs the names and times of authorized personnel entering and leaving SAP Fioneer's dedicated areas within the data centers.

2. SYSTEM ACCESS CONTROLS

Systems processing Data can only be accessed with authorization. SAP Fioneer protects its systems and controls access using the following means:

2.1 Multiple authorization levels are used when granting access to systems, including those processing Data. Authorizations are managed via defined processes.

2.2 All personnel access SAP Fioneer's systems using a personalized account (user ID).

2.3 Personnel have only access to the systems that they require to access in order to fulfill their duties. SAP Fioneer has procedures in place to implement the need-to-know principle for allowing system access. When personnel change their assigned role within the company, their access rights are timely revoked or adapted. As soon as personnel leave SAP Fioneer their access is revoked generally within 24 hours. SAP Fioneer uses authorization concepts that document grant processes and assigned roles per personalized account (user ID). Furthermore, authorization and privileges are reviewed on a regular basis.

2.4 SAP Fioneer has established a password policy that prohibits the sharing of personalized passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized accounts (user IDs) are assigned for authentication and must not be shared. All passwords fulfill defined minimum requirements, in particular for complexity and storage. Each end-user device has a password-protected screensaver.

2.5 The company network is protected from the public network by firewalls. SAP Fioneer operates an enterprise threat detection system to continuously and actively defend systems and infrastructure against attacks, using and analyzing audit logs.

2.6 SAP Fioneer uses up-to-date commercially available antivirus/malware protection software intended to prevent, detect and remove known malicious code. This includes signature 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.

2.7 Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to SAP Fioneer's corporate network and critical infrastructure is protected by strong authentication.

3. DATA ACCESS CONTROLS

Persons can access Data only according to their authorization. Data processed within the Services is classified as Confidential Information using the following means:

3.1 Access to Data is granted on a need-to-know basis. Personnel have access to the information that they require to access in order to fulfill their duties. When personnel leave or change their assigned role within the company, their access rights are timely revoked or adapted. As soon as personnel leave SAP Fioneer their access is revoked generally within 24 hours. SAP Fioneer uses authorization concepts that document grant processes and assigned roles per account (user ID). Furthermore, authorization and privileges are reviewed on a regular basis.

3.2 Data and data carriers are securely deleted or destroyed once they are no longer required. If hardware is removed from data centers a physical decommissioning process is applied.

3.3 Security measures that protect applications processing Data are regularly tested. To this end, SAP Fioneer conducts internal and external security checks and penetration tests on its IT systems.

3.4 SAP Fioneer has policies in place to prevent installations of not approved software on workstations and servers. Mobile devices and workstations shall be locked manually when left unattended. The screensaver is configured to automatically lock the screen within a maximum of five minutes of inactivity. This time-dependent lock of devices must not be deactivated.

3.5 Display screens for all systems that could disclose information allowing access to another SAP Fioneer 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.

3.6 Mobile devices that could provide access to devices or systems where Data is stored, have to be kept in the possession of personnel or locked in a secure location when not in use. Mobile devices must not be checked in as luggage when traveling.

4. DATA ENCRYPTION CONTROLS

SAP Fioneer applies the following measures to prevent Personal Data from being read, copied, modified or removed without authorization during transfer and at rest:

4.1 Data is encrypted at rest using market accepted standards

4.2 Data is encrypted using market accepted standards during transmission between secured networks in control of SAP Fioneer. Data in transfer over secured networks in control of SAP Fioneer is appropriately secured.

4.3 Mobile devices that could provide access to devices or systems where Data is stored use SAP Fioneer controlled network encryption when connecting to SAP Fioneer networks remotely.

4.4 For the transfer of Data between SAP Fioneer and its customers, SAP Fioneer will provide adequate protection measures for the transferred Data. The measures are defined in the product Documentation or otherwise in the Agreement. This applies to both physical and network-based data transfer. When data transfer is imitated by the Customer and/or encryption measures are under the Customer's control, the Customer is responsible for any such data transfer (e.g. data being transmitted outside the firewall of the SAP Fioneer data center). Customer is responsible for the physical transport (e. g. on movable media) outside of SAP Fioneer premises (e.g when provided to Customer's representative).

5. DATA INTEGRITY CONTROLS

SAP Fioneer applies the following measures to keep Data intact, complete and current during processing activities:

5.1 SAP Fioneer only allows authorized personnel to access Data as required in the course of their duty.

5.2 SAP Fioneer has implemented a system for logging and retaining SAP Fioneer's input, modification and deletion, or blocking of Data within the Cloud Service infrastructure.

5.3 Cloud Service applications provide logging systems for input, modification and deletion, or blocking of Data as described in the Documentation.

5.4 SAP Fioneer uses the technical capabilities of the deployed software (e.g. multi-tenancy, or separate system landscapes) to achieve data separation among Data originating from multiple customers.

5.5 The Data of the Customer (including its Controllers) is logically separated from Data of other customers. Access controls prevent the access of other customers to the Customer's Data.

5.6 For SAP Fioneer Support,

(a) SAP Fioneer customers have control over their remote support connections at all times. SAP Fioneer cannot access a Customer system without the knowledge and consent of the Customer. For SAP Fioneer Suppor, SAP Fioneer provides a specially designated, secure support ticket facility in which SAP Fioneer provides a special access-controlled and monitored security area for transferring access data and passwords. SAP Fioneer customers have control over their remote support connections at all times. SAP Fioneer employees cannot access a Customer on premise system without the knowledge and active participation of the Customer.

(b) If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

6. AVAILABILITY CONTROLS

Data is protected against accidental or unauthorized destruction or loss as follows:

6.1 SAP Fioneer employs regular backup processes to provide restoration of Data if and when necessary and provides disaster recovery services if expressly agreed for the respective Cloud Service.

6.2 SAP Fioneer uses uninterrupted power supplies (e.g. batteries, generators) for uninterrupted power availability to the data centers.

6.3 SAP Fioneer has implemented reasonable network connection bandwidths and Denial-of-Service (DoS) prevention measures for the data center providing the Cloud Service.

6.4 SAP Fioneer has defined business contingency plans for its own business-critical processes.

6.5 Emergency processes and systems including data recovery are regularly tested.

7. GOVERNANCE CONTROLS

Data is processed in accordance with the Agreement and related instructions of the Customer as follows:

7.1 SAP Fioneer uses controls and processes to monitor compliance with contracts entered between SAP Fioneer and its customers, subprocessors or other service providers respectively.

7.2 To process Data, SAP Fioneer and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. SAP Fioneer and its Subprocessors will regularly train personnel having access to Data in applicable data security and data privacy measures.