SAP Fieldglass

SOC 3 Report

Independent Practitioner's Trust Services Report For the SAP Fieldglass Solution System

For the Period of October 1, 2016, to September 30, 2017

Attestation and Compliance Services

schellman
Quality, above all.

INDEPENDENT PRACTITIONER'S TRUST SERVICES REPORT

To the Management of SAP America, Inc.:

We have examined management's assertion that during the period October 1, 2016, to September 30, 2017, SAP America, Inc. ("SAP Fieldglass") maintained effective controls over the SAP Fieldglass Solution system (the "system"), including controls over the privacy of personal information collected by the system for the security, availability, processing integrity, confidentiality, and privacy principles set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* (applicable trust services criteria), to provide reasonable assurance that

- the system was protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements;
- the system was available for operation and use to meet the entity's commitments and system requirements;
- system processing was complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements;
- information designated as confidential is protected to meet the entity's commitments and system requirements;
- personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements; and
- SAP Fieldglass complied with its commitments in its statement of privacy practices.

As indicated in the description, SAP Fieldglass uses various subservice organizations for data center hosting services and managed network and infrastructure services. The description indicates that certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organizations are suitably designed and operating effectively. The description presents SAP Fieldglass' system; its controls relevant to the applicable trust services criteria; and the types of controls that SAP Fieldglass expects to be implemented, suitably designed, and operating effectively at the subservice organizations to meet certain applicable trust services criteria, and compliance with the commitments in SAP Fieldglass' statement of privacy practices. The description does not include any of the controls expected to be implemented at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations, or their compliance with the commitments in their statement of privacy practices, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period October 1, 2016, to September 30, 2017.

SAP Fieldglass' management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the SAP Fieldglass Solution system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of SAP Fieldglass' relevant controls over the security, availability, processing integrity, confidentiality, and privacy of personal information of the SAP Fieldglass Solution system; (2) testing and evaluating the operating effectiveness of the controls; (3) testing compliance with SAP Fieldglass' commitments in its statement of privacy practices; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, SAP Fieldglass' ability to meet the aforementioned criteria and the commitments in its statement of privacy practices may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, in conformity with SAP Fieldglass' statement of privacy practices, based on the AICPA and CPA Canada applicable trust services criteria.

Schellman & Company, LLC

Tampa, Florida
November 6, 2017

MANAGEMENT'S ASSERTION

November 6, 2017

During the period October 1, 2016, to September 30, 2017, SAP America, Inc. ("SAP Fieldglass") maintained effective controls over the SAP Fieldglass Solution system (the "system"), including controls over the privacy of personal information collected by the system for the security, availability, processing integrity, confidentiality, and privacy principles set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* (applicable trust services criteria), to provide reasonable assurance that:

- the system was protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements;
- the system was available for operation and use to meet the entity's commitments and system requirements;
- system processing was complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements;
- information designated as confidential is protected to meet the entity's commitments and system requirements;
- personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements; and
- SAP Fieldglass complied with its commitments in its statement of privacy practices.

The attached system description identifies the aspects of the SAP Fieldglass Solution system covered by the assertion.

Daniel R. Bell
Senior Vice President, Technology

SYSTEM DESCRIPTION OF THE SAP FIELDGLASS SOLUTION SYSTEM

Company Background

SAP America, Inc. ("SAP Fieldglass") provides a cloud-based Vendor Management System (VMS) that enables organizations to procure, manage, and optimize their global external workforces, including contingent labor, freelancers, independent contractors, private talent pools, and services managed through Statements of Work (SOWs).

Headquartered in Chicago, Illinois, SAP Fieldglass has additional offices across the United States and in the United Kingdom, Australia, and India to serve its global customer base. SAP Fieldglass serves firms in more than 165 countries, and the solution is used in 20 languages by more than 85,000 staffing and service suppliers and more than sixteen million users.

SAP Fieldglass was founded in 1999 by Jai Shekhawat, an industry pioneer and recipient of the Ernst & Young Midwest Entrepreneur of the Year and Peter Yessne Staffing Innovator awards. Under his direction, SAP Fieldglass has been recognized by well-respected award programs including the American Business Awards, Illinois Technology Association CityLIGHTS Awards and CODiE Awards. For more information, visit www.fieldglass.com.

Description of Services Provided

SAP Fieldglass helps organizations achieve total workforce visibility, maximize cost savings, improve worker quality and enforce compliance. The enterprise platform offers a secure, private marketplace for a company and its chosen suppliers.

Companies use SAP Fieldglass to manage:

- Contingent labor across technology, healthcare/clinical, professional, creative, skilled trade and other specialized areas
- SOW-based projects and services
- Independent contractors and freelancers
- Specialized talent pools, such as retirees and alumni

The SAP Fieldglass platform may be used to perform a wide variety of functions that include, but are not limited to, the following:

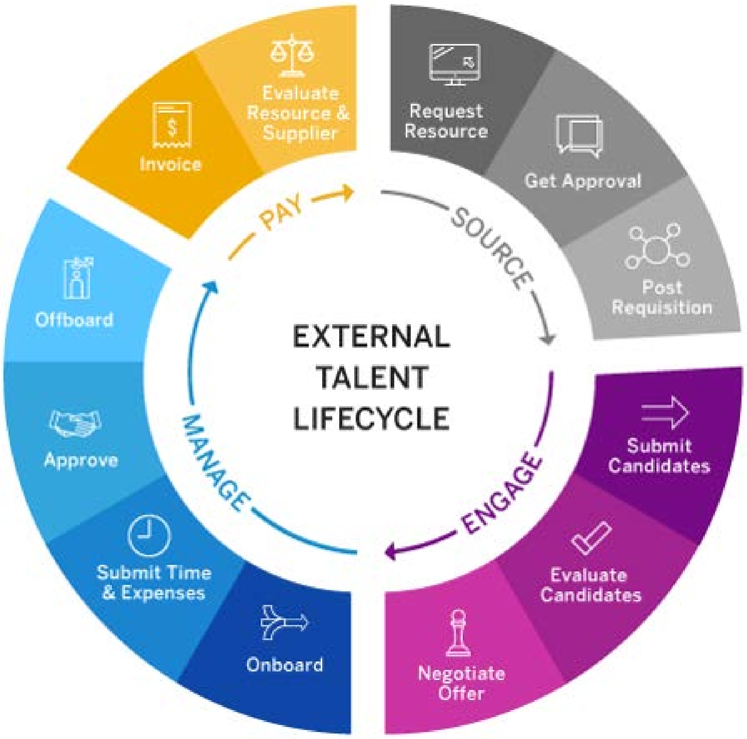
- Create, search, and archive requirements
- Generate preferred vendor lists
- Review resumes and rank candidates
- Schedule interviews
- Streamline on- and off-boarding processes
- Track and evaluate vendor and worker performance
- Create approval chains based on user profiles mapped to business rules
- Assign corporate authorization levels
- Produce detailed real-time reports
- Standardize job titles and pay according to a rate card
- Manage time and expense reports

- Automate invoicing, taxation and discounts
- Customize alerts and notifications

SAP Fieldglass Contingent

SAP Fieldglass' external workforce management module automates the entire process of procuring and managing flexible labor, from requisition all the way through invoice and payment. I t enables organizations to find, source and manage workers, enforce compliance, gain access to real-time data to better forecast costs, measure performance and plan for different types of labor needed in different scenarios. The platform supports any program model including those managed in-house, through one or more Managed Service Providers (MSPs) on- or off-site.

The diagram below illustrates the SAP Fieldglass Contingent process.

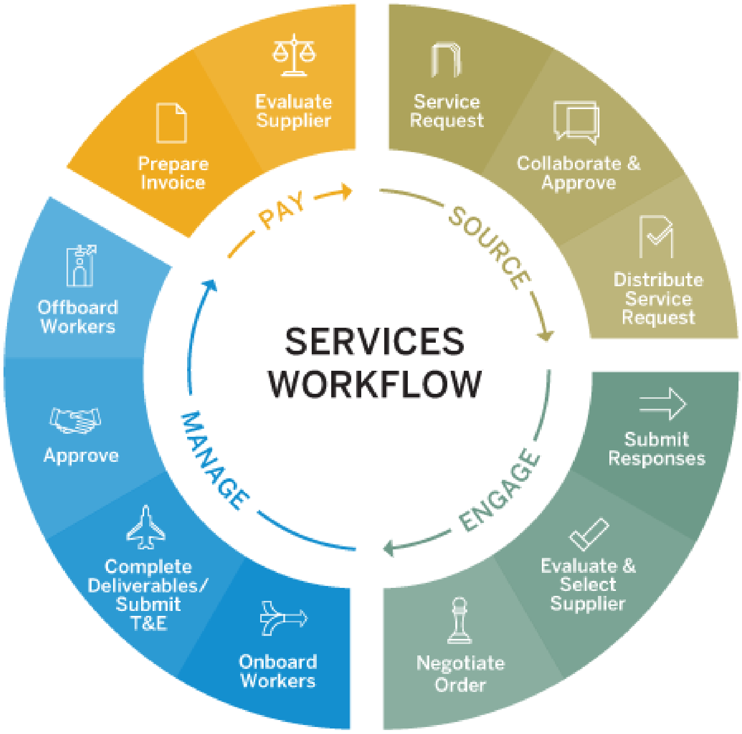


SAP Fieldglass Services Procurement

The SAP Fieldglass Services Procurement module streamlines the process of engaging third party service providers. It automates sourcing, contracting, purchasing, tracking, invoicing and payment for each project. SAP Fieldglass Services Procurement can accommodate any type of SOW, including unit-based, team-based, fixed-fee or Service Level Agreement (SLA)-based milestones.

[Intentionally Blank]

The diagram below illustrates the SAP Fieldglass Services process.



Benefits of Using SAP Fieldglass

Customers utilizing the SAP Fieldglass platform can:

- Drive users to the most appropriate engagement type for a given role or project
- Increase cost savings by bidding external services to preferred suppliers
- Control spend by enforcing the use of preferred suppliers and pre-defined rate cards
- Ensure the proper on- and off-boarding of external workers and service providers
- Increase the quality of the work and service being delivered by tracking vendor and worker performance, and level of effort
- Increase accuracy of time sheets and invoices
- Uncover critical insights with robust analytics and reporting to drive program improvements

Customer requests for services are initiated and authorized by user entities by directly contacting SAP Fieldglass. Customer requests are recorded and tracked by SAP Fieldglass through resolution, and are managed according to established contracted services and related SLAs.

Infrastructure and Software

The SAP Fieldglass application resides on physical servers and virtual machines. Production equipment is located in data centers operated by SAP SE ("SAP Corporate") in Rot, Germany, Cyxtera Data Centers, Inc. ("Cyxtera" or formerly CenturyLink) in Elk Grove, Illinois, and ServerCentral, Inc. ("ServerCentral") in San Jose, California, London, United Kingdom, and Amsterdam, Netherlands. The application is built on a J2EE architecture utilizing an n-tier approach. The application has a presentation layer for user interaction and rendering pages, a business layer for business rules and required validations, a service layer for delegation of persistence and workflow per business rules, and a persistence layer for persisting to the database.

The SAP Fieldglass Solution system is hosted in highly available infrastructure environments. Within the United States and Germany, SAP Fieldglass designs, deploys, manages, and is the owner of all production infrastructure from the cage in, including all hardware, devices, and software. Within the ServerCentral-operated facilities within the European Union (EU), ServerCentral manages the firewalls and configures the rules as requested by SAP Fieldglass. Additionally, ServerCentral manages the physical infrastructure; however, they are not provided with logical access to systems. Regardless of location, the hosting data center facilities provide Internet, heating, ventilation, air conditioning (HVAC), fire detection and suppression equipment, power, and physical security.

Components within the facilities are redundant, including firewalls, switches, network connectivity, database clusters, and content management appliances. Power is brought to the buildings through two entry point locations. This power is delivered to multiple power management modules that interconnect multiple battery storage systems and multiple generators. Infrastructure components have redundant power supplies and systems have multiple paths with infrastructure components spilt on a backplane.

SAP Fieldglass utilizes two redundant firewall pairs from two different vendors. The first firewall manages perimeter access. The second firewall manages inter-virtual local area network (VLAN) communications. Web servers are configured in a load balanced farm running Microsoft Windows operating systems and database servers are clustered in active-active mode.

Remote access is restricted to personnel via encrypted virtual private network (VPN) connections while access to the production environment is restricted to personnel already authenticated via remote desktop protocol (RDP) and two-factor authentication. VPN and RDP communication sessions are encrypted via various encryption protocols. To protect data in transit, transport layer security (TLS) encryption is utilized for web communication sessions.

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
SAP Fieldglass Application	Provides contingent workforce management solutions.	Microsoft Windows	Elk Grove, IL, San Jose, CA, London, United Kingdom, and/or Amsterdam, Netherlands
Active Directory	Used to manage user accounts, application access, and authentication requirements.	Microsoft Windows	Elk Grove, IL, San Jose, CA, London, United Kingdom, Amsterdam, Netherlands, and/or Rot, Germany
Firewalls / Switches	Used to filter and route traffic.	Cisco / FortiGate	Elk Grove, IL, San Jose, CA, London, United Kingdom, Amsterdam, Netherlands, and/or Rot, Germany
Virtual Hypervisor	Runs virtual machines for the execution of the operating system.	VMWare vCenter	Elk Grove, IL, San Jose, CA, London, United Kingdom, Amsterdam, Netherlands, and/or Rot, Germany
Servers	Used for virtual application delivery.	Microsoft Windows	Elk Grove, IL, San Jose, CA, London, United Kingdom, Amsterdam, Netherlands, and/or Rot, Germany

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
Databases	Used to store, retrieve, and manage data input into the system.	Microsoft Windows	Elk Grove, IL, San Jose, CA, London, United Kingdom, Amsterdam, Netherlands, and/or Rot, Germany

People

The personnel supporting the SAP Fieldglass Solution system include, but are not limited to, the following:

- Executive management – responsible for overseeing company-wide activities, establishing and accomplishing goals and overseeing objectives.
- Human resources (HR) – responsible for establishing policies, standards, and processes for recruitment, employee record-keeping, organizational design and development, and performance and behavior management.
- Systems administrators – responsible for functions such as patch management, antivirus/anti-malware administration, monitoring services, issue escalation and troubleshooting, and backup procedures.
- Virtualization system engineers – responsible for managing the virtualization environment under which the system operates.
- Network engineers – responsible for managing the network infrastructure.
- Developers – responsible for systems development and maintenance for in-house developed software.
- Quality assurance (QA) personnel – responsible for rigorously testing updates to the software before deployment to the production environment.

Procedures

Access Authentication and Authorization

Access to system information, including confidential data, is protected by authentication and authorization mechanisms. User authentication is required to access the production networks, including the application and database server operating system, the database, and the application. The information security policy outlines the formalized process for access provisioning, administration, and management.

Systems administration personnel are responsible for assigning and maintaining access rights to the production environment. In order to access the application or database server operating systems, users first authenticate to the network domain. Access to application and database server operating systems is governed by the primary domain controller’s policy. In order to access the production databases, users must authenticate to the database after they have authenticated to the database server.

Access Requests and Access Revocation

An automated provisioning process is in place for new hires. After the requested onboarding documentation is completed (nondisclosure agreement, background check, etc.), the candidate information is entered into a portal, in which the information is subsequently converted to an Excel spreadsheet and an automated script is run to create system access. A complex password is automatically assigned and the user account remains in a disabled state until activated. Once the HR department triggers an employee or contractor offboarding, automated tasks are sent to recipients for offboarding tasks including the creation of a checklist and subsequent termination of access. Systems administrators revoke system access privileges assigned to terminated employees as a component of the employee termination process. Escalations are sent to recipient’s managers and the security team when off-boarding tasks are not completed within expected timeframes. This escalation helps ensure employees and contractors do not retain system access subsequent to their termination date. The security team performs a review of access permissions on at least a quarterly basis to verify that network accounts are revoked for terminated employees and administrative access privileges are assigned to appropriate personnel.

Change Management

Internal personnel or customers can request a change via e-mail or verbal communication. Once a change request has been submitted, it is logged into a ticketing system. Change management personnel populate key fields, including the change request description, change type, priority, and target release. Changes are ultimately bundled into releases based on the following classifications:

- Major releases – major changes in functionality
- Minor releases – minor changes in functionality
- Service packs – small urgent changes

Releases follow a defined methodology for successful implementation, including the use of a change management system, detailed documentation to be completed, testing to be performed pre- and post-deployment, as well as approvals to be granted by various department leads including product development, QA, and professional services. However, major releases are subject to more stringent processes, including the completion of functional requirements that are required to be approved by project stakeholders, the documentation of detailed test plans and weekly test metrics prior to implementation, static code profiling to ensure secure coding standards are being adhered to, and penetration testing the application to help ensure vulnerabilities are addressed prior to implementation.

Development personnel execute unit test plans created by the QA team for major releases prior to releasing the software to QA for formal testing. QA personnel perform a vulnerability scan of the application for major releases to help ensure vulnerabilities are addressed prior to implementation, as well as regression and functional testing of major releases. Releases are implemented during scheduled maintenance windows. QA personnel perform post-deployment testing of change releases.

Formal quality gate meetings are conducted by the SAP Fieldglass release management team to ensure key performance indicators (KPIs), product requirements, and corporate requirements are being met throughout the systems development lifecycle (SDLC). Results are reviewed in a final decision gate meeting between SAP and the SAP Fieldglass release management team prior to deployment to the production environment.

Releases require an application digest to be generated to help ensure production code changes are authorized. This is performed before a release is deployed to production (to validate the state of the production environment) and after implementation (to validate that the certified code was deployed without modification). Additionally, application source code is escrowed within ten business days for releases. QA management performs a post-deployment escrow audit of change releases to help ensure that changes are escrowed within the specified timeframes.

Release management meetings are held on a weekly basis to discuss current and upcoming projects. In addition, the ability to implement changes into the production environment is restricted to authorized personnel.

<u>Version Control Software</u>

Version control software is utilized to manage versions of source code. The software allows development personnel to check-out different versions of the code for editing. Once users are ready to update the code repository, they check-in the version. The version control software assigns a different version number to each iteration and allows users to rollback code to previous versions when necessary. In addition, the software is configured to restrict code changes from being checked in without an associated change request. The ability to lock and unlock code within the version control software is restricted to authorized personnel.

Separation of Environments

Development and testing activities are performed in distinct environments that are physically and logically separate from production in order to ensure that changes made within the test environment do not affect changes in the production environment.

Patch Management

Patching is the process of installing a piece of software designed to fix problems and/or update a system. This includes fixing security vulnerabilities and other bugs and improving the usability or performance of a system. The patching process helps protect systems from vulnerabilities, such as viruses and/or malicious code. A patch management application is utilized to monitor, distribute, and apply patches to production servers. Scans of the production environments are performed on a monthly basis to identify security patches. A process for testing patches is in place – this process is formalized in regard to the production environment with documented approvals.

Patches are deployed during the scheduled maintenance windows to minimize the impact on the production environment. The ability to implement patches is restricted to authorized personnel via domain administration privileges.

Data Backup and Disaster Recovery

Production databases are backed up via an automated system – transaction logs are replicated between data center sites every 15 minutes and full database backups to local disk occur daily. At the conclusion of the full daily backup, the production database backups are replicated to the secondary data center, which is geographically separate from the primary data center. The automated backup and replication system is configured to notify systems administration personnel regarding the failure of relevant jobs, in which the cause is subsequently investigated. Additionally, restoration testing is completed on a monthly basis to help ensure data can be restored. The ability to retrieve production database backups from the off-site storage facilities is restricted to authorized personnel.

A disaster recovery plan is in place and the disaster recovery procedures are tested on an annual basis to help ensure that the contractually agreed upon recovery time and the recovery point objective from the time the disaster is officially declared by SAP Fieldglass senior management can be met.

Incident Response

The security team is designated to lead security incident investigations. Defined processes assign roles and responsibilities, address the reporting, classification, and handling of incidents, identify learning requirements from incidents, and the process for collection and retention of evidence. In addition, incidents are documented within a security incident report and are escalated, monitored, and reviewed as necessary. Incidents requiring a change to the system follow the standard change control process.

System Monitoring

The security team has configured security events to be logged according to internal prioritization. These security events consist of activities identified by the firewall and intrusion detection system (IDS). Events that are logged are sent to a centralized monitoring tool. The monitoring tool analyzes the log results and alerts security personnel via onscreen alerts in the event suspicious or unauthorized activities are identified. Upon receipt of the alerts, security personnel review the alerts to determine if any additional action should be taken.

An enterprise monitoring system is utilized to monitor the health and availability of the production environment. In the event that a monitored component falls out of the predefined monitoring thresholds, the enterprise monitoring application is configured to notify systems administration personnel via e-mail alerts. Once notified, systems administration personnel review the alerts and investigate the cause. Additionally, monthly performance metrics reports are generated for review by information technology (IT) management personnel to evaluate system performance and capacity requirements/needs. Windows production servers and workstations are protected by antivirus software, which is configured to update virus signature definitions on a daily basis. The antivirus software is configured to scan files upon access or modification.

SAP Fieldglass utilizes a vendor for help desk support during non-business hours and for customers that use other languages. This vendor is required to adhere to SAP Fieldglass' policies and procedures, including the privacy policy.

Data

The SAP Fieldglass application holds information such as job posting details, SOW details and related contractual clauses, rate card information, worker bill and pay rates, time sheet data, and invoices. The application, by design, does not require data that would require breach notifications, if compromised. If customers choose to store sensitive data, that may include Personally Identifiable Information (PII), custom fields may be defined that can be encrypted with advanced encryption standard (AES) 256-bit encryption. These fields can also be optionally masked from view while entering and viewing the fields in the application. Data can be delivered to users in various formats including the user interface, subscription-based reporting, job seeker resumes e-mailed to users, and e-mail approval requests. In addition, a native mobile application (iPhone/Android) is available for download that can be used to complete approval work items. SAP Fieldglass does not transmit personal information by mail or other physical means.

Data within the SAP Fieldglass application may be imported or exported via web services including simple object access protocol (SOAP) or representational state transfer (REST), SAP Fieldglass Integrator, hypertext transfer protocol secure (HTTPS), or secure file transfer protocol (SFTP)/file transfer protocol secure (FTPS) protocols. HTTPS transactions may be imported or exported either via the user interface or using SAP Fieldglass Integrator. SAP Fieldglass Integrator, which is a light-weight Java-based integration tool, can be used to integrate SAP Fieldglass with third party applications, such as enterprise resource planning (ERP) solutions. Additionally, many pre-built connectors are available for applications that include, but are not limited to, the following: PeopleSoft, Ariba, SAP, Oracle, SiteMinder, JD Edwards, Kronos, GEAC, Niku/Clarity, ADEO, Cyborg, and various legacy applications. SAP Fieldglass has developed various application programming interfaces (APIs) to facilitate integration to other enterprise applications and has architected both the SAP Fieldglass application and SAP Fieldglass Integrator to integrate to those applications.

The data within the SAP Fieldglass application is generated and uploaded by SAP Fieldglass' customers. Each customer is responsible for the accuracy and timeliness of data entered within the application and additionally has their own administrators which manage their users and data. Customer data stored within the system is considered confidential.

Significant Changes During the Review Period

No significant changes to the SAP Fieldglass Solution system occurred during the review period.

System Boundaries

As outlined in the 2016 TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* a system is designed, implemented, and operated to achieve specific business objectives (for example, delivery of services, production of goods) in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures and data.

Subservice Organizations

The data center hosting services provided by SAP Corporate, Cyxtera, and ServerCentral, and the managed network and infrastructure services for the production systems hosted within their European data centers provided by ServerCentral were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at SAP Corporate, Cyxtera, and

ServerCentral, alone or in combination with controls at SAP Fieldglass, and the types of controls expected to be implemented at SAP Corporate, Cyxtera, and ServerCentral to meet those criteria.

Control Activity Expected to be Implemented by SAP Corporate, Cyxtera, or ServerCentral	Applicable Trust Services Criteria
SAP Corporate, Cyxtera, and ServerCentral are responsible for ensuring controls are implemented to restrict physical access to facilities housing the system to authorized personnel.	CC5.5, PNC11
ServerCentral is responsible for configuring the firewall rules for their systems hosted within the EU as requested by SAP Fieldglass to block unauthorized inbound network traffic from the Internet.	CC5.6
ServerCentral is responsible for configuring and monitoring the IDS as requested by SAP Fieldglass and for alerting SAP Fieldglass of possible or actual security breaches for their systems hosted within the EU.	CC5.6
SAP Corporate, Cyxtera, and ServerCentral are responsible for ensuring controls are implemented to design, develop, implement, operate, maintain and monitor environmental protections.	A1.2, PI1.1

Statement of Privacy Practices

Within the SAP Fieldglass Solution system, SAP Fieldglass serves as the data processor; therefore, reliance is placed upon user entities (data controllers) for adherence to various privacy criteria.

User entities are responsible for providing their privacy notice to individuals. SAP Fieldglass communicates the privacy practices to user entities in the Statement of Privacy Practices. Therefore, the description does not address the (a)(i)(11) criteria in Section 2. The Statement of Privacy Practices includes the following, and is included below:

At SAP Fieldglass, we are committed to protecting your privacy. Please read the following policy to understand how your personal information will be treated as you make full use of our software and many services. Customers using the SAP Fieldglass application or other specialized applications developed or designed by SAP Fieldglass will be notified of updates to this policy in the release notes to the application. For customers using the SAP Fieldglass extranet or web sites, please check the site for changes from time to time.

I. Privacy Policy of SAP Fieldglass. We respect the privacy of our customers and are committed to treating customer information responsibly. Accordingly, we adhere to the following:

- We collect, retain, and use customer information for legitimate business purposes only. We limit the information we collect to that which we believe is appropriate and necessary to manage your needs, provide our services and comply with applicable law.
- We strive to maintain the accuracy of customer information.
- Our employees are responsible for protection of customer information. We have internal policies and programs designed to protect your information. It is the responsibility of each SAP Fieldglass employee to comply with our privacy policies and procedures.
- We provide security safeguards to protect customer information. Multiple security layers, including sensor and host based intrusion detection along with firewalls, protects all customer data. All customer data that is taken off site uses Advanced Encryption Standard (AES).

- We limit the internal and external disclosure of customer information. Other than as set forth herein, SAP Fieldglass does not sell, trade or rent your personal information. To opt to not have your personal information shared as set forth herein, contact us at +(1) 312.763.4800; provided, however that to the extent you are a registered user of the SAP Fieldglass application, your personal information is a requirement and removal of your personal information will result in termination of your user account (i.e., termination of your ability to use the SAP Fieldglass application). We may share with our partners' and customers' non-personal, aggregate statistical information regarding you, your customers, your suppliers, sales, traffic patterns and site usage, but we do not share personally identifiable information with any entity that is not covered by this policy.

II. The Information We Collect. We rely on many sources of information to help us understand and meet your needs. On occasion, we enter into agreements with other vendors to provide services in support of the SAP Fieldglass services; currently, SAP Fieldglass utilizes another organization for help desk support services for the SAP Fieldglass application. We carefully stipulate under these agreements that these vendors may view personal information about you, and that they must protect this information and may not use it for any other purpose other than in connection with our agreement and otherwise in accordance with your instructions and this privacy policy.

We may collect personal information about you including:

- Information about your transactions with us, our affiliates or nonaffiliated third party users of the SAP Fieldglass application.
- Information we receive about you from applications and other forms, which we have collected by your using products or services obtained from us, one of our affiliates or nonaffiliated third party users of the SAP Fieldglass application.
- Information about you as required or permitted by law.
- Your name and other contact details when you call us by phone, write to us or contact us using our website or establish a user account for the SAP Fieldglass application.
- Information about you when you apply for a job or contract with us (for example, your name and contact details, information about your working history and relevant records checks).
- Information we receive from our customers and other third party users of our application. For example, we collect information relating to individuals' job applications from the entities who use the SAP Fieldglass application (for example, companies and their consulting and recruitment agencies). The SAP Fieldglass application is used by companies to manage their workforces. Companies may ask that their agencies also use the application so that these entities can exchange information relating to job candidates between one another. SAP Fieldglass collects this personal information by virtue of hosting the application. The information SAP Fieldglass collects may include sensitive information, such as personal data your employer has deemed relevant for employment-related or record keeping purposes, where you provide that information to us or to the entities that use the SAP Fieldglass application.
- Information about you if you are an individual who is, or who is employed by, one of our suppliers, contractors, related companies, agents and customers. For example, SAP Fieldglass may collect the personal information of the employees or contractors of the entities who use its application.

III. Why Do We Collect Information? SAP Fieldglass collects the personal information it needs to provide services and information to its customers, for its business operations and to comply with the law. Depending on the circumstances, SAP Fieldglass may also use personal information about you to:

- Accurately identify you.
- Protect and administer your records and accounts.
- Help us notify you of product enhancements and changes to products.
- Save you time when you apply for additional products and services.
- Comply with certain laws and regulations.
- Collect information about the usage of our services.

- Respond to your requests for information about our services.
- Assist us in our decision on whether or not to make you an offer of employment or engage you under a contract.

If you choose not to provide certain personal information to us, we may not be able to provide you with the services or information you require.

IV. How Do We Collect Your Information? SAP Fieldglass collects information related to you in several ways:

- Some personal information is gathered when you register. The more information you volunteer (and the more accurate it is), the better we are able to customize your experience.
- In addition to the above, we may also ask you for personal information at other times, including (but not limited to) when you enroll in a program offered by one of our partners, when you alter your request for services (i.e., increase your annual spend) and when you report a problem with our software or one of our services. If you contact SAP Fieldglass we may keep a record of that correspondence. SAP Fieldglass may also occasionally ask you to complete surveys that we use for research purposes.
- As noted above, we may also collect your information from third party users of the SAP Fieldglass application. For example, we collect information relating to individuals' job applications from entities that use the SAP Fieldglass application.

V. How is the Collected Information Used?

- We may monitor usage to help us develop upgrades to the software and develop the design and layout of the website.
- We may also use the information we collect to occasionally notify you about important functionality changes and special offers we think you'll find valuable.
- SAP Fieldglass collects, stores and uses information from the users of its application (meaning the computer software programs), and the hosted environment (meaning a hardware/software system combination under the control of SAP Fieldglass on which the Product, or any portion thereof, is run). Aggregated versions of this information (information that does not personally identify you) may be used in many ways. For example, we may combine information about your usage patterns, with similar information obtained from other users to help enhance the application or hosted environment and our services. Additionally, SAP Fieldglass may keep track of this information and the information that you provide to us for our internal review, business development, research, press inquiries or aggregate statistical analysis, customization, demographic patterns, and historical trends. Aggregate information may occasionally be shared with our business partners and customers, and this information does not include any personally identifiable information about you or allow anyone to identify you individually. As SAP Fieldglass adopts additional technology we may also gather information through other means.

VI. Disclosing Personal Information. For the purposes described in this policy, we may disclose personal information:

- To any of our related companies;
- To our suppliers, contractors and service providers, professional advisers, dealers and agents;
- To government agencies or individuals appointed by a government responsible for the investigation and resolution of disputes or complaints concerning use of our services;
- To anyone to whom our assets or business (or any part of it) is transferred or offered to be transferred;
- Where you have otherwise consented; or
- As otherwise required or authorized by law.

We may disclose personal information to recipients outside of the United States, the United Kingdom and Australia. Such recipients are likely to be located in the jurisdictions in which we have corporate offices – for example, our main headquarters are located in the United States, with related companies located in the United

Kingdom and Australia. We take reasonable steps to ensure the persons and organizations to whom we disclose personal information are bound to protect the privacy of that personal information in accordance with applicable law.

VII. Information Security. We restrict access to personal information about you to those who need to have that information to provide products or services to you. If we use other companies to provide products or services to you, we require that they keep the information we share with them safe and secure. We have physical, logical and procedural safeguards in place that comply with legal requirements to store and secure information about you from unauthorized access, alteration and destruction. We remind you, however, that the internet is not a secure environment and although all care is taken, we cannot guarantee the security of information that you provide via the SAP Fieldglass application.

VIII. Cookies and IP Address Tracking. The SAP Fieldglass website may use cookies for site administration purposes. If for any reason you wish not to take advantage of cookies, you may have your browser not accept them, although this may disable or render unusable some of the features of the SAP Fieldglass application.

SAP Fieldglass' website may also detect and use your IP address or domain name for internal traffic monitoring and capacity purposes or to otherwise administer the application. No personal information is obtained; rather the patterns of usage of visitors to the website may be tracked for the purposes of providing improved service and content based on aggregate or statistical review of user site traffic patterns.

The SAP Fieldglass application may contain links to other websites. SAP Fieldglass is not responsible for the privacy practices or the content of such other websites. The privacy policies applicable to such other websites may differ substantially from this privacy policy so we advise you to read them before using those websites. SAP Fieldglass will not be liable for any use of those websites.

IX. Consent. By using the SAP Fieldglass application, you consent to the collection, use and disclosure of this information, including any sensitive information, by SAP Fieldglass. If we decide to change our privacy policy, we will post those changes in this document so that you are always aware of what information we collect, how we use it, and under what circumstances we disclose it. SAP Fieldglass reserves the right, at any time, to modify, alter or update these policies. This policy is effective as of June 26, 2002 and may be modified from time to time. In the event you have any inquiries regarding these privacy matters, please contact us at +(1) 312.763.4800.

SAP Fieldglass is a participant in the Safe Harbor programs developed by the U.S. Department of Commerce with the European Union and with the Federal Data Protection and Information Commission of Switzerland. SAP Fieldglass has certified that we adhere to the Safe Harbor Privacy Principles with regard to our use of certain personal data. For more information about Safe Harbor and to view our certification, visit the U.S. Department of Commerce's Safe Harbor Web site. http://www.export.gov/safeharbor.

SAP Fieldglass is aware of the decision of the European Court of Justice involving the “Safe Harbor” framework and has taken the necessary steps to remain in compliance with its obligations under applicable data privacy laws and regulations. Despite changes in applicable law, Fieldglass is committed to maintaining robust data privacy and data security controls in order to protect each individual’s right to privacy, including working with Customers to address country-specific regulations and continuing to uphold the privacy principles required for self-certification under Safe Harbor. If you have any specific questions or concerns, please feel free to reach out directly to fieldglass_privacy@sap.com.

X. Additional Provisions. Access, Correction and Complaints Handling. Any issues, questions, complaints that you have regarding the access, correction and/or handling of your information must be addressed with your employer’s administrator of the SAP Fieldglass application.

Destruction of Personal Data. SAP Fieldglass retains personal information for only as long as necessary to fulfil the stated purposes or as required by law or regulation. Thereafter, except in the event of a governmental audit, investigation, or pending litigation, records containing personal data are destroyed by either deleting them from electronic files (including back-up and archived files) or properly disposing (such as in a shredder or document destruction repository) hard copies and electronic media such as disks or backup tapes.

Further Information. If you would like further information about our privacy policies or practices please contact our Privacy Officer:

SAP Fieldglass

E-mail: fieldglass_privacy@sap.com
111 North Canal Street
Suite 600 Chicago, Illinois, 60606
United States