Security Exhibit

Workday maintains a comprehensive, written information security program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of Workday's business; (b) the amount of resources available to Workday; (c) the type of information that Workday will store; and (d) the need for security and confidentiality of such information.

Workday's security program is designed to:

- Protect the confidentiality, integrity, and availability of Customer Data or Professional Services Data in Workday's possession or control or to which Workday has access;
- Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Customer Data or Professional Services Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Customer Data or Professional Services Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data or Professional Services Data; and
- Safeguard information as set forth in any local, state or federal regulations by which Workday may be regulated.

Without limiting the generality of the foregoing, Workday's security program includes:

1. **Security Awareness and Training**. A mandatory security awareness and training program for all members of Workday's workforce (including management), which includes:

   a) Training on how to implement and comply with its Information Security Program;

   b) Promoting a culture of security awareness through periodic communications from senior management with employees.

2. **Access Controls**. Policies, procedures, and logical controls:

   a) To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;

   b) To prevent those workforce members and others who should not have access from obtaining access; and

   c) To remove access in a timely basis in the event of a change in job responsibilities or job status.

3. **Physical and Environmental Security**. Controls that provide reasonable assurance that access to physical servers at the production data center or the facility housing Workday's SFTP Server, if applicable, is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes. These controls include:

   a) Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;

   b) Camera surveillance systems at critical internal and external entry points to the data center;

   c) Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and

   d) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

4. **Security Incident Procedures**. A security incident response plan that includes procedures to be followed in the event of any Security Breach. Such procedures include:

   a) Roles and responsibilities: formation of an internal incident response team with a response leader;

b) Investigation: assessing the risk the incident poses and determining who may be affected;

c) Communication: internal reporting as well as a notification process in the event of unauthorized disclosure of Customer Data or Professional Services Data;

d) Recordkeeping: keeping a record of what was done and by whom to help in later analysis and possible legal action; and

e) Audit: conducting and documenting root cause analysis and remediation plan.

5. **Contingency Planning**. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Customer Data or production systems that contain Customer Data. Such procedures include:

   a) Data Backups: A policy for performing periodic backups of production file systems and databases or Professional Services Data on Workday's SFTP Server, as applicable, according to a defined schedule;

   b) Disaster Recovery: A formal disaster recovery plan for the production data center, including:

      i) Requirements for the disaster plan to be tested on a regular basis, currently twice a year; and

      ii) A documented executive summary of the Disaster Recovery testing, at least annually, which is available upon request to customers.

   c) Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

6. **Audit Controls**. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information.

7. **Data Integrity**. Policies and procedures to ensure the confidentiality, integrity, and availability of Customer Data or Professional Services Data and protect it from disclosure, improper alteration, or destruction.

8. **Storage and Transmission Security**. Security measures to guard against unauthorized access to Customer Data or Professional Services Data that is being transmitted over a public electronic communications network or stored electronically. Such measures include requiring encryption of any Customer Data or Professional Services Data stored on desktops, laptops or other removable storage devices.

9. **Secure Disposal**. Policies and procedures regarding the secure disposal of tangible property containing Customer Data or Professional Services Data, taking into account available technology so that Customer Data or Professional Services Data cannot be practicably read or reconstructed.

10. **Assigned Security Responsibility**. Assigning responsibility for the development, implementation, and maintenance of its Information Security Program, including:

    a) Designating a security official with overall responsibility;

    b) Defining security roles and responsibilities for individuals with security responsibilities; and

    c) Designating a Security Council consisting of cross-functional management representatives to meet on a regular basis.

11. **Testing**. Regularly testing the key controls, systems and procedures of its information security program to validate that they are properly implemented and effective in addressing the threats and risks identified. Where applicable, such testing includes:

    a) Internal risk assessments;

b) ISO 27001 and ISO 27018 certifications; and

c) Service Organization Control 1 (SOC1) and Service Organization Control 2 (SOC2) audit reports (or industry-standard successor reports)

12. Monitoring. Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes:

a) Reviewing changes affecting systems handling authentication, authorization, and auditing;

b) Reviewing privileged access to Workday production systems; and

c) Engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

13. Change and Configuration Management. Maintaining policies and procedures for managing changes Workday makes to production systems, applications, and databases. Such policies and procedures include:

a) A process for documenting, testing and approving the patching and maintenance of the Service;

b) A security patching process that requires patching systems in a timely manner based on a risk analysis; and

c) A process for Workday to utilize a third party to conduct web application level security assessments. These assessments generally include testing, where applicable, for:

i) Cross-site request forgery

ii) Services scanning

iii) Improper input handling (e.g. cross-site scripting, SQL injection, XML injection, cross-site flashing)

iv) XML and SOAP attacks

v) Weak session management

vi) Data validation flaws and data model constraint inconsistencies

vii) Insufficient authentication

viii) Insufficient authorization

14. Program Adjustments. Workday monitors, evaluates, and adjusts, as appropriate, the security program in light of:

a) Any relevant changes in technology and any internal or external threats to Workday or the Customer Data or Professional Services Data;

b) Security and data privacy regulations applicable to Workday; and

c) Workday's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

15. Devices. All laptop and desktop computing devices utilized by Workday and any subcontractors when accessing Customer Data or Professional Services Data:

a) will be equipped with a minimum of AES 128 bit full hard disk drive encryption;

b) will have up to date virus and malware detection and prevention software installed with virus definitions updated on a regular basis; and

c) shall maintain virus and malware detection and prevention software so as to remain on a supported release. This shall include, but not be limited to, promptly implementing any applicable security-related enhancement or fix made available by supplier of such software.

Definitions

"Professional Services" means consulting or professional services provided to Customer under an agreement between the parties for the provision of consulting or professional services, including but not limited to the following agreements or terms: the Lifecycle Deployment Program Terms and Conditions, the Professional Services Agreement, the Delivery Assurance terms, the Professional Services Addendum, and/or the Consulting and Training Addendum and Amendment.

"**Professional Services Data**" means electronic data or information that is provided to Workday under a Professional Services engagement with Workday for the purpose of being input into the Workday Service, or Customer Data accessed within or extracted from the Customer's tenant to perform the Professional Services.

"**SFTP Server**" means a Secure File Transfer Protocol server or its successor provided and controlled by Workday to transfer the Professional Services Data between Customer and Workday for implementation purposes.