Workday security and data privacy

Introduction

As business becomes increasingly digital, securing and protecting customer, employee, and intellectual property data is a top priority for IT leaders. And with organisations facing more sophisticated security threats, it's critical to deliver security and data privacy across all aspects of service. Here is an introduction to Workday practices across security and data privacy for IT professionals.

Regulatory compliance and certifications

Workday and our customers must comply with various international privacy regulations. Common privacy principles throughout jurisdictions include notice, choice, access, use, disclosure, and security. Our application is designed to allow you to achieve differentiated configurations so you can obey your country's specific laws.

Workday also achieves compliance with international privacy regulations by maintaining a comprehensive, written information-security programme that contains technical and organisational safeguards designed to prevent unauthorised access to and use or disclosure of customer data.

External audits: SOC 1 and SOC 2 reports

The operations, policies, and procedures at Workday are audited regularly to ensure that Workday meets and exceeds all standards expected of service providers. Workday publishes a Service Organisation Controls 1 (SOC 1) Type II report. The SOC 1, which is the successor to the SAS 70, is issued in accordance with the Statement on Standards for Attestation Engagements No. 18 (SSAE 18) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402).

This dual-standards report gives companies around the world confidence that the service provider, such as Workday, has the appropriate controls in place. The intended audience for this report is a customer or prospect who is required to have an understanding of internal controls over outsourced critical business tasks that have an impact on a customer's financial statements (Sarbanes-Oxley compliance). The scope of the SOC 1 is limited to Workday production systems, and the SOC 1 audit is conducted every six months by an independent third-party auditor. The report is available to customers and prospects upon completion.

Workday also publishes a Service Organisation Controls 2 (SOC 2) Type II report. The Workday SOC 2 report addresses all trust services principles and criteria (security, availability, confidentiality, processing integrity, and privacy). The scope of the SOC 2 covers any Workday system that contains data that the customer submitted to Workday Services. The intended audience for this report is a customer or prospect who is interested in understanding Workday internal security controls. The SOC 2 audit is conducted once a year by an independent third-party auditor and is available to customers or prospects upon completion.

Both the SOC 1 and the SOC 2 audits validate Workday physical and environmental safeguards for production data centres, backup and recovery procedures, software development processes, and logical security controls.

ISO 27001, 27017, and 27018 Certifications

ISO 27001 is an information security standard originally published in 2005 by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). In September 2013, ISO 27001:2013 was published, and it supersedes the original 2005 standard.

ISO 27001 is a globally recognised, standards-based approach to security that outlines requirements for an organisation's information security management system (ISMS).

ISO 27017, published in 2015, is a complementary standard to ISO 27001. This standard provides controls and implementation guidance for information security applicable to the provision and use of cloud services.

ISO 27018 is a complementary standard, published by ISO/IEC in 2014, that contains guidelines applicable to cloud service providers that process personal data.

Workday achieved certification against ISO 27001 in September 2010, ISO 27018 in October 2015, and ISO 27017 in November 2017. Certification is achieved following an independent assessment of Workday conformity to the ISO standard. ISO recertification occurs every three years, but to maintain certification, a business must go through annual surveillance audits. These ISO certifications affirm our commitment to privacy and security and demonstrate that our controls are operating effectively. The ISO certificates and ISMS Statement of Applicability are available for customer review.

Cross-border data transfers

Strict data protection laws govern the transfer of personal data from the European Economic Area (EEA) to the United States. To address this requirement for our customers with operations in the EEA, Workday has incorporated the European Commission's approved standard contractual clauses, also referred to as the "Model Contract," into our Data Protection Agreement. The Model Contract creates a contractual mechanism to meet the adequacy requirement to allow for transfer of personal data from the EEA to a third country.

Workday is also self-certified for the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield. The Privacy Shield replaces the Safe Harbour Framework and is intended to specifically address issues that the European Court of Justice identified in its ruling invalidating the Safe Harbour Framework. Workday is an active Privacy Shield participant. TRUSTe is used as the Workday third-party verification method for the Privacy Shield.

More information about the U.S. Department of Commerce's Privacy Shield programme can be found at http://www.privacyshield.gov. More information on the Standard Contractual Clauses can be found at http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

Additional information on the Workday commitment to safeguarding the privacy of our customers' data and details of our privacy programme can be found in the Workday Privacy Programme datasheet.

The General Data Protection Regulation

The General Data Protection Regulation (GDPR), a European Union (EU) regulation, repeals and replaces Data Protection Directive 95/46/EC as well as the implementing legislation of the member states. This regulation took effect in all 28 EU member states on 25 May 2018, and simplifies and harmonises current data protection laws in all EU member states. The GDPR applies to companies in the EU as well as all companies that process or store the personal data of EU citizens, regardless of their location.

Workday is a data processor as defined under the GDPR. Workday has comprehensively evaluated GDPR requirements and implemented numerous privacy and security practices to ensure data processor compliance with GDPR from day 1. These practices include:

- Training employees on security and privacy practices
- Conducting privacy impact assessments
- Providing sufficient data transfer methods to our customers
- Maintaining records of processing activities
- Providing configurable privacy and compliance features to our customers

Privacy by design and privacy by default are concepts deeply enshrined in Workday Services. Because we recognise that the GDPR is a critical business priority for our global customers, Workday continues to monitor guidance that EU supervisory authorities issue on the GDPR to ensure that our compliance programme remains up-to-date.

Data security

Physical security

Workday co-locates its production systems in state-of-the-art data centres designed to host mission-critical computer systems with fully redundant subsystems and compartmentalised security zones. Workday data centres adhere to the strictest physical security measures:

- Multiple layers of authentication are required before access is granted to the server area.
- Critical areas require two-factor biometric authentication.
- Camera surveillance systems are located at critical internal and external entry points.
- Security personnel monitor the data centres 24/7.
- Unauthorised access attempts are logged and monitored by data centre security.

All physical access to the data centres is highly restricted and stringently regulated. Workday data operations use security best practices such as "least access" hardened servers and regularly scheduled maintenance windows.

Data segregation

Workday is a multi-tenant SaaS application.

Multi-tenancy is a key feature of Workday that enables multiple customers to share one physical instance of the Workday system while isolating each customer tenant's application data. Workday accomplishes this through the Workday Object Management Server (OMS). Every user ID is associated with exactly one tenant, which is then used to access the Workday application.

All instances of application objects (such as Organisation and Worker) are tenant-based, so every time a new object is created, that object is also irrevocably linked to the user's tenant. The Workday system maintains these links automatically and restricts access to every object, based on the user ID and tenant. When a user requests data, the system automatically applies a tenancy filter to ensure that it retrieves only information corresponding to the user's tenant.

Encryption of data at rest (database security)

Workday encrypts every attribute of customer data within the application before it is stored in the database. This is a fundamental design characteristic of the Workday technology. Workday relies on the Advanced Encryption Standard (AES) algorithm with a key size of 256 bits. Workday can achieve this encryption because it is an in-memory object-oriented application as opposed to a disk-based RDBMS application. Specifically, metadata in Workday is interpreted by the Workday OMS and stored in memory. All data inserts, updates, and deletes are committed to a persistent store on a MySQL database. This unique architecture means Workday operates with only a few dozen database tables. By contrast, a RDBMS-based application requires tens of thousands of tables, making complete database encryption impractical due to its detrimental impact on performance.

Encryption of data in transit (network security)

Users access Workday via the internet, protected by Transport Layer Security (TLS). This secures network traffic from passive eavesdropping, active tampering, and forgery of messages.

Workday has also implemented proactive security procedures, such as perimeter defence and network intrusion prevention systems. Vulnerability assessments and penetration testing of the Workday network infrastructure are also evaluated and conducted on a regular basis by both internal Workday resources and external third-party vendors.

Data backups

The Workday primary production database is replicated in real time to a replica database maintained at an off-site data centre. A full backup is taken from this replica database each day. Our database backup policy requires database backups and transaction logs to be collected so that a database can be recovered with the loss of as few committed transactions as is commercially practicable. Transaction logs are retained until there are two backups of the data after the last entry in the transaction log. Database backups of systems that implement interfaces must be available as long as necessary to support the interfacing systems. This period will vary by system. Backups of the database and transaction logs are encrypted for any database that contains customer data.

Disaster recovery

Workday warrants its service to its standard service-level agreement (SLA). The SLA includes a disaster recovery (DR) plan for the Workday Production Service with a recovery time objective (RTO) of 12 hours and a recovery point objective (RPO) of 1 hour. The RTO is measured from the time the Workday Production Service becomes unavailable until it is available again. The RPO is measured from the time the first transaction is lost until the Workday Production Service became unavailable.

To make sure Workday maintains these SLA commitments, Workday maintains a DR environment with a complete replication of the production environment. In the event of an unscheduled outage where the outage is estimated to be greater than a predefined duration, Workday executes its DR plan. The DR plan is tested at least every six months.

One security model

Unlike legacy ERP systems, Workday operates on a single security model. This includes user access, system integration, reporting, mobile devices, and IT access. Everyone must log in and be authorised through the Workday security model. By contrast, in legacy ERP systems, there typically is an applications layer of security that IT and DBA personnel can bypass to access the data directly at the database level. This is not possible with Workday. Workday is an object-oriented in-memory system with an encrypted persistent data store. As a result, access events and changes are tracked and audited. This uniquely robust security model, combined with the automatic ability to effectively date and audit all data updates, shortens the time and lowers the costs associated with governance and compliance and reduces overall security risk.

Authentication

Workday security access is role-based, supporting SAML for single-sign-on (SSO) and x509 certificate authentication for both user and web services integrations. Workday allows customers to set up different authentication requirements for different user populations.

Workday also enables users to select an authentication type in situations where organisations wish to use multiple authentication types for users, due to geographical and/or organisational variances.

Single-sign-on support

While LDAP allows for a unified username/password solution, SAML takes the next step by enabling an enterprise SSO environment. SAML allows for a seamless SSO experience between the customer's internal identity and access management (IAM) solution and Workday.

Workday native login

For customers who wish to use the native login, Workday stores their Workday password only in the form of a secure hash, rather than the password itself. Unsuccessful login attempts as well as successful login/logout activity are logged for audit purposes. Inactive user sessions are automatically timed out after a specified time, which is customer-configurable by user. Customer-configurable password rules include length, complexity, and expiration.

Multifactor authentication

Workday provides and recommends that customers use multifactor authentication (MFA). Workday allows customers to supply any authenticator application backed by the Time-Based One-Time Passcode (TOTP) algorithm. With this setup, customers can easily integrate MFA providers with the Workday native login. Workday also allows end users of customers to receive a one-time passcode delivered via an email-to-SMS gateway mechanism. Lastly, Workday supports challenge questions as an additional mechanism to prove a user's identity.

Trusted devices

Workday provides the ability for customers and their end users to enrol devices as trusted for access to their Workday tenant. End users will be notified of unrecognised devices attempting to access their account. They will have the ability to remove devices they no longer trust. For administrators, a list of trusted devices is provided for monitoring purposes. To configure this feature, administrators need to enable it for their tenant and end users must consent to tracking of the trusted device with a browser cookie.

Step-up authentication

Workday provides step-up authentication as a stronger authentication mechanism for access to sensitive resources. Organisations using SAML as an authentication type can further ensure that data is secured against unauthorised access to items within Workday deemed critical. This allows customers to force a secondary authentication factor that users must enter to access those items.

Authorisation

The Workday application enforces group policy-based security for authorisation. The application prevents any user from directly accessing the production database. Workday-delivered and customer-created security groups, combined with predefined security policies, grant or restrict user access to functionality, business processes, reports, and data – whether accessed online or through web services.

Customer-configurable security groups are based on users, roles, jobs, organisations, location hierarchy, or business sites. They can be combined into new security groups that logically include and exclude other groups. System-to-system access is defined by integration system security groups. Customers can tailor these groups and policies to meet their needs, providing as fine-grained access as required to support complex configurations, including global implementations.

Workday also provides security groups that are automatically updated on the basis of business processes, such as hire and end contract. These Workday-delivered groups can be used alone or in combination with other Workday-delivered or customer-created security groups to determine access via security policies.

Public cloud

Workday uses public cloud services from Amazon Web Services (AWS) for storing and processing content in Workday Media Cloud. Customer content is logically segregated from that of other customers. All Workday Media Cloud content is encrypted at rest, using AWS's server-side encryption. Each object Workday stores within AWS is encrypted with AES with a unique 256-bit encryption key.

Workday uses Amazon Virtual Private Cloud (Amazon VPC), which is a logically isolated section of the AWS cloud. All communication between end users to Workday data centres and Workday Amazon VPC services is encrypted at the transport layer. Additionally, all of the communication from Workday Amazon VPC services to Workday data centres and vice versa is encrypted as well. Workday uses the TLS protocol to encrypt all the traffic with secure ciphers only.

Always-on auditing

Workday tracks all changes to business data at the application level. This application audit information is the basis for audit and compliance reporting found throughout the Workday system. Workday records successful logins and logouts by users as well as unsuccessful login attempts and provides this information in Workday audit reports. Workday uses non-destructive updates, which means data is never overwritten and is maintained for the lifetime of the tenant. This enables customers to obtain a complete audit history of any value. The auditing features in Workday provide an auditor with the information required to trace the history of changes made to a business object or transaction.

About Workday

Workday is a leading provider of enterprise cloud applications for finance and human resources.

Founded in 2005, Workday delivers financial management, human capital management, and analytics applications designed for the world's largest companies, educational institutions, and government agencies. Organisations ranging from medium-sized businesses to *Fortune* 50 enterprises have selected Workday.

workday.

Workday | Phone: +44 (0)20 3318 2336 | workday.com/uk