Privacy overview

Quick Reference Guide

Workday Privacy Overview

Access to Workday information is for job related purposes only. Workday data is confidential and is used solely for the purpose of providing human resources, workforce development, learning management and budget functions internal to the state. Workday is expected to expand to include payroll.

Workday utilizes security groups and roles, combined with system security policies to grant or restrict user access to protected information, functionality, business processes, reports, documents and data. Agency employees and contingent workers with elevated security access, acknowledge and adhere to strict confidentiality conditions outlined within the Workday Security Agreement document. Additionally, only employees and contingent workers authorized by their supervisors are able to access protected information. Agencies utilize the Security Role Descriptions to determine the appropriate role assignments based on workers' responsibilities.

The Workday Worker Document Types describes data classification levels and the roles that can add or view documents.

All employees can view the workers assigned to the elevated roles that support their organization. See: Find Your Support Roles

Organization and Employee Information

Employees in Workday can view all organizational structures within Workday. For more information, please reference the job aid: Search Organizations. Employees can also view basic information about the employees within the selected organization.

Employees, other than those previously mentioned, cannot view information that is private or sensitive. This information includes, but is not limited to: Information protected under the definition of Personally Identifiable Information (PII), protected worker data, personal contact information, bank account information, withholding elections, military documentation, medical information, performance reviews, disciplinary actions, race/ ethnicity, gender, gender identity, and disability status.

System Use Tracking and Auditing

Workday is designed to track and audit all events and changes that are made. Data cannot be overwritten, which allows Workday security auditors to obtain a complete audit history of transactions.

Processes are in place to identify areas of potential data conflicts or compromises and are regularly monitored by the Workday team. Events that pose any risk to data privacy are thoroughly researched, acted upon accordingly, and documented.

Additional Information: For information regarding Workday delivered security provided by Workday, Inc., see Workday Security and Data Privacy.