# Workday Security Standard

## Introduction

This document sets forth a comprehensive framework designed to protect sensitive user data and ensure secure operations within the Workday environment. Workday, a cloud-based enterprise platform, is used for managing human resources, talent, learning and payroll, and it processes critical information that requires stringent protection. By implementing authorization, identification and authentication controls, access to the Workday platform is restricted to authorized users only. Using authorization, identification and authentication controls ensures that only those users have access to the Workday platform.

## Purpose

To establish a comprehensive security framework for the use, management and integration of Workday within OMES and affiliated state agencies. This standard ensures the confidentiality, integrity and availability of sensitive data processed through Workday.

## Standard

Personal information security.

- Enhanced security measures are implemented for personal information prompts, report fields and tasks, ensuring a consistent user experience when handling sensitive data.

Data access security.

- Workday focuses on configurable security to protect data access. This includes transparent communication about data protection practices.

User-based security roles – a type of security group that grants access privileges directly to a specific user, rather than assigning permissions based on their job, organization or location.

- Continuous improvements are made to audit role-based security, allowing easier access to see security roles for workers and role assigners, as well as the ability to create custom reports.
- Audits to the security groups happen every 90 days.

Integration security.

- The security model for integrations includes:
    - Access control – Different security domains manage permissions for configuring and running integrations.
    - Data access – Integrations access Workday data through secure web service operations and must have appropriate permissions for report data sources and fields.
    - External endpoint security – Workday provides encryption and signature options to secure data transmitted to external systems.

Proxy security access.

- Proxy access in Workday allows a user to temporarily act on behalf of another user within the system. It is typically used for testing, troubleshooting or administrative purposes, especially in non-production environments.

- Proxy access is limited to HR and payroll team members. Any requests for access outside these roles require approval from the agency HR director.
- Every proxy access must be approved by the agency decentralized security representative (DSR).
- Proxy access is limited to each agency's own data.
- Proxy access is reviewed every six months.

These measures collectively ensure that Workday maintains a high standard of security for its users and their data.

**Compliance**
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

**Rationale**
To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

**Revision history**
This standard is subject to periodic review to ensure relevancy.

| | |
|---|---|
| **Effective date:** 09/15/2025 | **Review cycle:** Annual |
| **Last revised:** 09/15/2025 | **Last reviewed:** 09/15/2025 |
| **Approved by:** Dan Cronin, Chief Information Officer | |