



Identity and Access Management Standard

DOC-IT-IS-32
Revision 1.1
APRIL 9, 2026

This document contains proprietary information, which is the exclusive property of RXO, Inc. and may not be used or reproduced, in whole or in part, without the express permission of RXO, Inc.

Copyright © 2026 RXO, Inc. All rights reserved.

REVISION HISTORY

This revision history lists all changes to this document, the date of each revision, and the reason for each revision.

<u>Rev.</u>	<u>Rev. Date</u>	<u>Revision Description</u>
1.0	11/01/2025	Initial Version
1.1	4/9/2026	Additional requirements added

Table of Contents

32	Identity and Access Management Standard.....	4
32.1	Executive Summary.....	4
32.2	Purpose	4
32.3	Scope	4
32.4	Identity and Access Management Standard Statements	4
32.4.1	Principles.....	4
32.4.2	Identity Lifecycle Management.....	5
32.4.3	Authentication	5
32.4.4	Authorization and Access Control.....	5
32.4.5	Monitoring and Auditing.....	6
32.4.6	Training.....	7
32.5	Roles and Responsibilities.....	7
32.6	Compliance	7
32.7	Exceptions.....	7
32.8	Review & Updates.....	7
32.9	References	7
32.10	Definitions	8

32 Identity and Access Management Standard

32.1 Executive Summary

This standard highlights the technological and procedural areas that RXO will address to affect a comprehensive Identity and Access Control approach as a key preventative control in RXO's Information Security Strategy. The objective is to ensure that all users have authorized access rights in accordance with the requirements of their role.

This standard defines the identity access control requirements surrounding the management of access to information assets on RXO's enterprise network as well as those assets residing in RXO cloud-based solutions.

32.2 Purpose

The purpose of this standard is to establish the requirements necessary to ensure that access to and use of RXO's information resources are managed in accordance with business requirements, security best practices, and applicable laws and regulations (e.g., GDPR, HIPAA, CMMC, SOX).

32.3 Scope

This standard applies to RXO, Inc., including all subsidiaries, divisions, and operating entities. All directors, officers, full-time and part-time employees, agents, contractors, and third parties acting on behalf of RXO must comply with this standard. It includes systems, applications, end user computing devices, and network resources within RXO. It covers the entire lifecycle of an identity, from provisioning to deprovisioning.

32.4 Identity and Access Management Standard Statements

32.4.1 Principles

The Identity and Access Management (IAM) program at RXO is based on the following core principles:

Need-to-Know: Access shall be granted only to the specific resources required to perform assigned job functions.

Least Privilege: Users shall be granted the minimum level of access necessary to perform their tasks.

Separation of Duties: Access privileges shall be designed to prevent a single individual from controlling multiple stages of a critical business process.

Accountability: All access and related activities shall be logged, monitored, and auditable.

32.4.2 Identity Lifecycle Management

The complete lifecycle of a digital identity must be managed through documented processes for onboarding, role changes, and offboarding.

Provisioning (Joiners): Access shall be granted upon employment/engagement and role assignment, following the necessary approvals.

Role Changes (Movers): Access rights and permissions shall be updated promptly when personnel change roles or responsibilities, removing outdated permissions and applying new ones as needed.

Deprovisioning (Leavers): All access shall be revoked immediately upon termination of employment or engagement. Regular audits shall be conducted to identify and disable orphaned accounts.

32.4.3 Authentication

All users must verify their identity before accessing resources.

Central Authentication: Centralized identity providers shall be used wherever possible to enable Single Sign-On (SSO) and consistent policy enforcement.

Multi-Factor Authentication (MFA): Use of an InfoSec approved MFA platform is required for all personnel accessing critical systems, sensitive data, and for all remote access and privileged accounts. An Infosec approved MFA platform is required for all carriers (external accounts) accessing public RXO systems. Logging is required for the MFA platform.

Password Management: Personnel must adhere to the RXO Password Policy, which defines requirements for complexity, length, and rotation. Credentials are not to be saved in browsers.

Non-Human Identities: Non-human entities (e.g., service accounts, machines, applications) must have their identities and access managed securely, with appropriate authentication mechanisms (e.g., API keys, certificates).

32.4.4 Authorization and Access Control

Access to resources shall be controlled based on defined policies.

Role-Based Access Control (RBAC): RBAC shall be the primary method for defining and assigning permissions based on job functions. Roles must be clearly defined and documented. Nested group access may not be used.

Access Policies: Access policies shall be based on data sensitivity, user roles, and contextual factors (location, device, time). Other than public facing applications, access to RXO networks, systems, applications, and data will be limited to RXO managed devices which meet Information Security standards for security controls and patching managed through Intune. Non RXO managed systems (AKA Vendor owned and supplied) will NOT be authorized to directly access RXO systems,

applications, and data. When approved by InfoSec, access will be provisioned through Infosec approved platforms such as VDI or Z-Scaler.

Privileged Access Management (PAM): All privileged access to servers, databases, or systems will be performed with ADM accounts, not with standard user accounts. Privileged accounts shall be subject to enhanced controls, including dedicated processes, session monitoring, and just-in-time (JIT) access mechanisms to minimize standing privileges. All Privileged accounts will be onboarded, managed, and accessed through CyberArk Privilege Cloud. Admin accounts cannot be granted e-mail or Internet access unless an exception is requested in ServiceNow and approved by InfoSec. Highly Privileged accounts will be separated as a different identity from a normal ADM account. Examples include Global Admin, Enterprise Admin, Schema Admin, Intune Admin, etc. No local accounts with elevated privileges will be allowed on workstations, VDIs, or servers without a documented, time-bound exception approved by Infosec. Users will not have Local Admin Rights on workstations or VDI's without a documented, time-bound exception approved by Infosec.

Access Reviews: Periodic reviews of user access rights shall be conducted by resource owners to ensure permissions remain appropriate and aligned with current roles. Access reviews for privileged accounts should be conducted more often than other accounts, at least quarterly, preferably monthly.

Shared Accounts: The use of shared accounts in general is prohibited, and when needed must be requested as an exception via ServiceNow and approved by InfoSec. Examples include default accounts on vendor systems that cannot be disabled that may have critical functionality for the platform. Shared Accounts will be onboarded, and access shared, via CyberArk WPM (the password will not be shared).

Service Accounts: Service Accounts are only to be used for Non-Interactive Login access, not for standard user login. Key authentication must be used for service accounts. Keys must be maintained in an InfoSec approved secure vault with access limited and regularly reviewed. API Service Keys will be stored in an InfoSec approved vaulted location and rotated every 12 months. Service accounts cannot be granted e-mail or Internet access unless an exception is requested in ServiceNow and approved by InfoSec.

32.4.5 Monitoring and Auditing

Continuous monitoring and auditing are essential for accountability and security.

Logging: All successful and failed authentication attempts and significant access events (e.g., privilege escalation, access to sensitive data) shall be logged.

Auditing: Access logs and system activities shall be regularly reviewed to detect suspicious activity, ensure policy adherence, and provide audit trails for compliance.

Incident Response: Identified security incidents related to IAM shall be handled according to the RXO Incident Response Plan.

32.4.6 Training

Training: All personnel shall receive regular training on IAM policies, security best practices, and their role in protecting company data.

32.5 Roles and Responsibilities

Approving Authority: Ensures overall compliance with this standard.

IAM Team/IT Administrators: Manages the IAM systems, including user provisioning, account maintenance, and monitoring.

Resource/System Owners: Defines access criteria for their systems and data, approves access requests, and conducts regular access reviews.

All Personnel: Must comply with this standard and related policies; any violation may result in disciplinary action.

32.6 Compliance

The IAM program shall be aligned with all applicable regulatory and compliance requirements. Non-compliance with this standard may result in access restrictions to affected systems or disciplinary actions as per RXO's guidelines.

32.7 Exceptions

Any exceptions to this standard must be requested in ServiceNow and approved in writing by the RXO Governance Risk and Compliance (GRC) team. Requests must include a valid business justification.

32.8 Review & Updates

This standard will be reviewed annually, or upon major infrastructure or threat landscape changes, or as required due to changes in business or technical requirements.

32.9 References

- RXO Access Management Policy

- RXO Password Management Standard
- RXO Security Incident Response Policy

32.10 Definitions

IAM	Identity and Access Management
SSO	Single Sign-on
MFA	Multi-Factor Authentication
RBAC	Role-Based Access Control
PAM	Privileged Access Management
GRC	Governance, Risk and Compliance

Certificate of Review

Identity and Access Management Standard

July 2nd 2026 2:09:08 pm

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Thursday, April 16, 2026 2:08 PM EDT
Faisal Khan		Policy Approver	Approved	Tuesday, June 30, 2026 12:27 PM EDT
Mark Gutman		Policy Admin	Published	Thursday, July 2, 2026 2:09 PM EDT