



Data Governance Standard

DOC-IT-IS-35
Revision 1.0
JANUARY 27, 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	01/27/2026	Initial Version

Table of Contents

35 Data Governance Standard	4
35.1 Executive Summary	4
35.2 Purpose	4
35.3 Scope	4
35.4 Data Governance Standard Statements	4
35.4.1 Data Classification	4
35.4.2 Data Storage	5
35.4.3 Data Access Controls.....	5
35.4.4 Data Retention	5
35.4.5 Data Disposal.....	6
35.4.6 Data Processing.....	6
35.4.7 Compliance with Regulations.....	6
35.5 Roles & Responsibilities.....	7
35.5.1 Information Owners (Operations).....	7
35.5.2 Application Teams.....	7
35.5.3 Database Teams.....	7
35.5.4 Identity Management Team	7
35.5.5 Platform Server Teams	7
35.5.6 EUC Team	7
35.5.7 Integration Team.....	8
35.6 Compliance	8
35.7 Exceptions.....	8
35.8 Review & Updates.....	8
35.9 References	8
35.9.1 RXO References.....	8
35.9.2 External References.....	8
35.10 Definitions.....	9

35 Data Governance Standard

35.1 Executive Summary

This document provides a comprehensive approach to manage and protect RXO and customer data throughout its lifecycle to ensure effective management, security, and integrity of the data, reducing the risk of losing the confidence of our customers to financial penalties. The standard includes data storage, processing, and compliance with policies and regulations.

35.2 Purpose

The purpose of this document is to define standards related to data governance to mitigate risk related to data misuse or inaccuracies, to promote practices that enhance accuracy, consistency, and reliability of data, and to ensure adherence to legal and regulatory requirements.

35.3 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 policy.

35.4 Data Governance Standard Statements

35.4.1 Data Classification

- 35.4.1.1 All Company Information must be classified, protected, and destroyed in accordance with the RXO Information Classification Standard.
- 35.4.1.2 Information owners are responsible for classifying the information in their data information repositories and documenting the data classifications for all data, all data sources, and all data shared with partners.
- 35.4.1.3 Information that has not yet been classified must be treated as Confidential. Refer to the Information Classification Definitions in the Information Classification Standard.
- 35.4.1.4 Information must be labeled in accordance with its classification. Refer to the Information Classification Labeling Standards in the Information Classification Standard.
- 35.4.1.5 Information must be protected and handled in accordance with its classification. Refer to the Information Classification Handling Standards in the Information Classification Standard.
- 35.4.1.6 The classification and handling of duplicated, printed, copied, or reproduced information must remain consistent with the original information.

- 35.4.1.7 Information containing differing Classification Levels must be classified at the most restrictive applicable Classification Level.

35.4.2 Data Storage

- 35.4.2.1 The RXO Cryptography Policy must be followed to ensure the protection of data at rest and in transit.
- 35.4.2.2 Cryptographic controls must be in place to achieve information security objectives, including the use of encryption of information to protect the confidentiality of information that is sensitive or classified.
- 35.4.2.3 Procedures must be included to address the appropriate use of encryption for protection of information during transmission and by mobile or removable media devices or across communication lines.
- 35.4.2.4 RXO must implement, and maintain processes, procedures, and controls to protect data and ensure the required level of continuity for information security during an adverse situation following the RXO Disaster Recovery and Business Continuity Policy.

35.4.3 Data Access Controls

- 35.4.3.1 All provisions of the RXO Access Control Policy must be followed to manage user access provisioning and deprovisioning to approve or deny access requests to systems, applications, networks, and network services.
- 35.4.3.2 Users must only be provided access to systems, applications, networks, and network services that are required to perform their assigned job duties.
- 35.4.3.3 Access controls must be implemented for systems, applications, networks, and network services to enforce role-based access provisioning and management.
- 35.4.3.4 Privileged access rights must be controlled and specifically allocated to accounts and users based on approved roles and the concept of Least Privilege and need-to-know.
- 35.4.3.5 Privileged access rights must be assigned to a user account different from those used for regular business activities; regular business activities must not be performed using privileged user accounts.
- 35.4.3.6 Access to systems and applications must be controlled by a secure log-on procedure that does not display passwords.

35.4.4 Data Retention

- 35.4.4.1 All systems owners must follow the RXO Data Retention Policy.
- 35.4.4.2 Data must be retained for as long as necessary to fulfill legal, regulatory, contractual, and operational obligations.
- 35.4.4.3 Data should be securely disposed of once retention periods expire.

- 35.4.4.4 Data must be protected against unauthorized access, loss, alteration, and destruction during its retention period.
- 35.4.4.5 Data must be stored in encrypted, access-controlled environments.
- 35.4.4.6 Backup data must be protected and follow identical retention rules.
- 35.4.4.7 Archival storage must ensure integrity, availability, and confidentiality.
- 35.4.4.8 If a litigation hold, investigation, or audit is underway, relevant data must not be deleted or altered until authorized.
- 35.4.4.9 All exceptions must be documented and approved by Legal Counsel and the Information Security Officer.

35.4.5 Data Disposal

- 35.4.5.1 Data must be disposed of following the RXO Data Retention Policy.
- 35.4.5.2 Upon expiration of the retention period, data must be securely destroyed.
- 35.4.5.3 Digital data: Secure erase, degaussing, or crypto shredding. For Government data, disposal must follow the NIST SP 800-88 Media Sanitization guidelines.
- 35.4.5.4 Physical documents: Cross-cut shredding, pulping, or incineration
- 35.4.5.5 Disposal must be documented, and certificates of destruction retained where applicable.

35.4.6 Data Processing

- 35.4.6.1 Every effort should be made to standardized how data is entered into systems to maintain uniformity (standardize data formats).
- 35.4.6.2 Appropriate data validation measures should be taken to ensure the accuracy and consistency of data.
- 35.4.6.3 RXO should not collect sensitive data from customers or other partners unless it is required to perform the services defined in our contract.
- 35.4.6.4 RXO should only share the minimum information required with partners to enable them to perform the services for which they are hired.

35.4.7 Compliance with Regulations

- 35.4.7.1 Where RXO is a government contractor or sub-contractor receiving Controlled Unclassified Information (CUI), RXO must follow the NIST SP 800-171, Protecting Controlled Unclassified Information, for all in-scope assets. Information owners should contact InfoSec for assistance.
- 35.4.7.2 Where RXO is a government contractor or sub-contractor receiving non-public information, but not CUI, that information is Federal Contract Information (FCI), RXO

must follow the Federal Acquisition Regulations, FAR 52.204-21. Information owners should contact InfoSec for assistance.

- 35.4.7.3 Where RXO will receive Protected Health Information (PHI), RXO must follow HIPAA guidelines. Information owners must consult with RXO Legal.
- 35.4.7.4 Where RXO will receive information covered under the GDPR, such as when dealing with customers or partners in the European Union, RXO must follow the GDPR guidelines in the GDPR Applicability Reference Standard. Information owners must consult with RXO Legal.

35.5 Roles & Responsibilities

35.5.1 Information Owners (Operations)

- 35.5.1.1 Ensure the data classification, labeling and handling requirements in this standard and the RXO Information Classification Standard are followed.
- 35.5.1.2 Ensure that data classifications are known, understood, and documented.
- 35.5.1.3 Engage InfoSec for any government contract or subcontract.
- 35.5.1.4 Engage RXO Legal for any HIPAA or GDPR contracts.

35.5.2 Application Teams

- 35.5.2.1 Ensure the data classification, access control, data retention, disposal and processing rules in this standard are followed.

35.5.3 Database Teams

- 35.5.3.1 Follow data storage and retention rules and ensure data at rest is encrypted following this standard and the RXO Cryptography Policy.

35.5.4 Identity Management Team

- 35.5.4.1 Ensure user provisioning and deprovisioning rules in this standard and the RXO Access Control Policy are followed.

35.5.5 Platform Server Teams

- 35.5.5.1 Ensure the data storage and disposal rules in this standard and the RXO Disaster Recovery and Business Continuity Policy are followed.

35.5.6 EUC Team

- 35.5.6.1 Ensure the data disposal rules in this standard are followed.

35.5.7 Integration Team

- 35.5.7.1 Follow the data classification and processing rules in this standard and ensure the RXO Cryptography Policy is followed for encryption of data in transit.

35.6 Compliance

Non-compliance with this policy may result in access restrictions to affected systems or disciplinary actions as per RXO's guidelines.

35.7 Exceptions

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

35.8 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.

35.9 References

35.9.1 RXO References

- 35.9.1.1 RXO Information Classification Standard
- 35.9.1.2 RXO Cryptography Policy
- 35.9.1.3 RXO Disaster Recovery and Business Continuity Policy
- 35.9.1.4 RXO Access Control Policy
- 35.9.1.5 RXO Data Retention Policy
- 35.9.1.6 RXO Acceptable Use Policy
- 35.9.1.7 RXO Privacy Policy
- 35.9.1.8 RXO California Residents Privacy Policy
- 35.9.1.9 GDPR Applicability Reference Standard

35.9.2 External References

- 35.9.2.1 NIST SP 800-81 Media Sanitization

- 35.9.2.2 NIST SP 800-171 Protecting Controlled Unclassified Information
- 35.9.2.3 FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems
- 35.9.2.4 HIPAA Administrative Simplification Rules - 45 CFR Parts 160-164

35.10 Definitions

NIST SP	National Institute of Standards and Technology Special Publication
CUI	Controlled Unclassified Information
FCI	Federal Contract Information
FAR	Federal Acquisition Regulations
CFR	Code of Federal Regulations
PHI	Protected Health Information
HIPAA	Health Insurance Portability and Accountability Act
GDPR	General Data Protection Regulation

Certificate of Review

Data Governance Standard

March 24th 2026 12:09:45 pm

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Tuesday, January 27, 2026 3:59 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, March 24, 2026 11:07 AM EDT
Mark Gutman		Policy Admin	Published	Tuesday, March 24, 2026 12:09 PM EDT