



Security Compliance Policy

DOC-IT-IS-18
Revision 2.1
NOVEMBER 1, 2025

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 © 2025 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	11/01/2022	Initial Version
2.0	11/01/2024	Annual Review
2.1	11/01/2025	RXO, Inc updates, annual review

18.0 Security Compliance Policy

18.0.1 Purpose

18.0.1.1 The purpose of the RXO, Inc. (RXO) Security Compliance Policy is to provide information security requirements for the processes related to RXO's legal, regulatory and contractual compliances and information security reviews.

18.0.2 Scope

18.0.2.1 This policy applies to all RXO subsidiaries, divisions, and operating entities, all employees, agents, contractors, and third-party partners, as well as all data and systems used by or supporting the company.

18.1 Compliance with Legal and Contractual Requirements

18.1.1 Identification of Applicable Legislation and Contractual Requirements

18.1.1.1 All relevant legislative statutory, regulatory, contractual requirements and RXO approach to meet these requirements must be explicitly identified, documented, and kept up to date for each information system and RXO.

18.1.1.1.A Those RXO personnel responsible for compliance must identify all specific legislative requirements that are applicable to their organization according to the type or line of business. Managers must also consider compliance in all relevant countries, if/as applicable.

18.1.1.1.B A centralized compliance registry must be maintained, detailing all applicable legislative, statutory, regulatory, and contractual requirements. This registry must be regularly reviewed and updated to capture any changes in regulatory environments or new business areas.

18.1.2 Intellectual Property Rights

18.1.2.1 RXO must ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products. Specific control areas that RXO must consider are:

- Acquiring software only through known and reputable sources;
- Maintaining awareness of policies to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them;
- Maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights;
- Maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.;
- Complying with the terms and conditions for software and information obtained from public networks;

- Not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law; and
- Not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.

18.1.3 Protection of Records

18.1.3.1 Records must be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual, and business requirements.

18.1.3.1.A Technical, procedural and process changes must include an evaluation of the information security continuity, whether in an operational or continuity context.

18.1.3.1.B Protection of specific organizational records must consider the corresponding classification based on the appropriate classification scheme. Records should be categorized into record types with details of retention periods and type of allowable storage media. Any related cryptographic keys and programs associated with encrypted archives or digital signatures must also be stored to enable decryption of the records for the length of time the records are retained.

18.1.3.1.C The storage of records procedures and controls must evaluate the possibility of deterioration in accordance with manufacturer's recommendations.

18.1.3.1.D Electronic storage media procedures must be in place to ensure the ability to access data throughout the retention period to safeguard against loss due to future technology changes.

18.1.3.1.E Data storage systems must support data retrieval in an acceptable timeframe and format, depending on the business requirements.

18.1.3.1.F An inventory of sources of key information must be maintained.

18.1.3.1.G Storage and handling procedures must contain retention, storage, handling and disposal of records, information guidelines, and retention schedules identifying records and the period of time they must be retained. The system must permit appropriate destruction of records after that period if no longer necessary.

18.1.4 Privacy and Protection of Personally Identifiable Information

18.1.4.1 Privacy and protection of personally identifiable information must be ensured as required in relevant legislation and regulation where applicable.

18.1.4.1.A RXO must govern the handling and protection of personally identifiable information or other privacy-related assets. This policy must be communicated to all persons involved in the processing of personally identifiable information.

18.1.4.1.B Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of personally identifiable information must be managed by a Privacy Officer, including specific procedures and guidance for managers, users and service providers on their individual responsibilities.

18.1.4.1.C The governance for handling personally identifiable information and ensuring awareness of the privacy principles must comply with relevant legislation and regulations and

support appropriate technical and organizational measures to protect personally identifiable information.

18.1.4.1.D Privacy Impact Assessments (PIAs) must be conducted whenever new systems or processes handling PII are introduced to identify and mitigate potential privacy risks.

18.1.5 Regulation of Cryptographic Controls

18.1.5.1 Cryptographic controls must be used in compliance with all relevant agreements, legislation, and regulations.

18.1.5.1.A Compliance requirements for relevant legislation and regulations must be determined before encrypted information or cryptographic controls traverse across jurisdictional borders, as applicable. This should be determined through pre-defined practices or legal consultations.

18.2 Information Security Reviews

18.2.1 Independent Review of Information Security

18.2.1.1 RXO will regularly review information security controls through the use of independent 3rd parties, internal audit and targeted reviews by SMEs at least annually.

18.2.2 Compliance with Security Policies and Standards

18.2.2.1 Managers must regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

18.2.2.1.A If any non-compliance is found as a result of a review, managers must identify the causes of noncompliance; evaluate the need for actions to achieve compliance; implement appropriate corrective action; review the corrective action taken to verify its effectiveness; and identify any deficiencies or weaknesses.

18.2.2.1.B Results of reviews and corrective actions carried out by managers must be formally documented and made available for review and reference as required.

18.2.3 Technical Compliance Review

18.2.3.1 Information systems must be regularly reviewed for compliance with RXO's information security policies and standards.

18.2.3.1.A Technical compliance of systems and applications with information security policies and standards must be provided via sufficient evidence of accuracy and completeness. Whenever possible, these reviews should be performed with the assistance of automated tools, with the generation of technical reports for subsequent interpretation by a technical specialist. Alternatively, manual reviews, supported by appropriate software tools, if necessary, by a competent system/software engineer can be used if an equivalent level of detail is made available.

18.2.3.1.B Penetration tests must occur, at least annually, and must be planned, documented, and consistently executed to prevent any compromise of the security of the system. Iterative vulnerability assessments must be planned, documented, and consistently executed to prevent any compromise of the security of the RXO network.

18.2.3.1.C Any technical compliance review must only be carried out by competent, authorized persons, or under the supervision of such persons.

Certificate of Review

Security Compliance Policy

December 18th 2025 10:30:20 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 3:41 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:00 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:30 AM EST