



Supplier Relationships Policy

DOC-IT-IS-15
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 Revision
2.1	11/01/2025	RXO, Inc updates, annual review

15.0 Supplier Relationships Policy.....	4
15.0.1 Purpose.....	4
15.0.2 Scope	4
15.1 Information Security in Supplier Relationships	4
15.1.1 Information Security for Supplier Relationships.....	4
15.1.2 Addressing Security within Supplier Agreements.....	4
15.1.3 Information and Communication Technology Supply Chain	5
15.2 Supplier Service Delivery Management.....	5
15.2.1 Monitoring and Review of Supplier Services	5
15.2.2 Managing Changes to Supplier Services	5

15.0 Supplier Relationships Policy

15.0.1 Purpose

15.0.1.1 The purpose of the RXO, Inc. (RXO) Supplier Relationships Policy is to define information security requirements for the processes related to contractual supplier relationships and supplier service delivery management.

15.0.2 Scope

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

15.0.2.2 This policy encompasses security with supplier agreements, information and communication technology supply chain and monitoring and reviewing of supplier services.

15.0.2.3 This policy applies to all information assets and other classes of protected information.

15.1 Information Security in Supplier Relationships

15.1.1 Information Security for Supplier Relationships

15.1.1.1 Information security requirements for mitigating the risks associated with supplier's access to the organization's assets must be agreed with the supplier and documented.

15.1.1.1.A Information security controls must be implemented to specifically address supplier access to RXO's data. These controls must comprise processes and procedures requiring implementation by RXO, as well as those processes and procedures that RXO requires the supplier to implement.

15.1.1.1.B RXO must maintain a Third-Party Risk Management Program to assess, monitor, and manage risks associated with suppliers. The program includes an initial risk assessment, ongoing monitoring, and annual security reviews to ensure suppliers continue to meet RXO'S security requirements.

15.1.1.1.C Supplier agreements must specify data protection standards, including compliance with data privacy laws (e.g., GDPR, CCPA) and data encryption requirements. This includes a mandate for suppliers to have processes for securely deleting RXO'S data when no longer needed.

15.1.2 Addressing Security within Supplier Agreements

15.1.2.1 All relevant information security requirements must be established and agreed to by each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

15.1.2.1.A Supplier agreements must be established and documented to ensure that there is no misunderstanding between RXO and the supplier regarding both parties' obligations to fulfill relevant information security requirements.

15.1.3 Information and Communication Technology Supply Chain

15.1.3.1 Agreements with suppliers must include requirements to address the information security risks associated with information and communications technology services and product supply chain.

15.2 Supplier Service Delivery Management

15.2.1 Monitoring and Review of Supplier Services

15.2.1.1 Organizations must regularly monitor, review and audit supplier service delivery.

15.2.1.1.A Monitoring and reviewing of supplier services must be conducted to ensure that the information security terms and conditions of the agreements comply with the requirements and that information security incidents and problems are managed in accordance with the requirements.

15.2.1.1.B A designated individual or service management team must be assigned the responsibility for managing supplier relationships. In addition, suppliers must be assigned responsibilities for reviewing compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources must be available to monitor that the requirements of the agreement, in particular to evaluate if the information security requirements are being met.

15.2.1.1.C Appropriate action must take place when deficiencies in the service delivery occur.

15.2.1.1.D A process must be developed, documented, and implemented to ensure that RXO retains sufficient overall control and visibility into all security aspects for all information or information processing facilities accessed, processed, or managed by a supplier. RXO must also retain visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting and response through a defined reporting process.

15.2.2 Managing Changes to Supplier Services

15.2.2.1 Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures, and controls, must be managed, taking into account the criticality of business information, systems, and processes involved and re-assessment of risks.

15.2.2.1.A When managing changes to supplier agreements consideration must be given to changes made by RXO to implement enhancements to the current services offered, development of any new applications and systems, modifications or updates of the organization's policies and procedures and new or changed controls to resolve information security incidents and to improve security.

15.2.2.1.B When managing changes to supplier services consideration must be given to changes in supplier services to implement, changes and enhancement to networks, use of new technologies, adoption of new products or newer versions/releases, new development tools and environments, changes to physical location of service facilities, change in suppliers and sub-contracting to another supplier.

Certificate of Review

Supplier Relationships Policy

December 18th 2025 10:27:16 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 4:24 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 10:59 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:27 AM EST