



Communications Security Policy

DOC-IT-IS-13
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

Table of Contents

13.0 Communications Security Policy.....	4
13.0.1 Purpose.....	4
13.0.2 Scope	4
13.1 Network Security Management.....	4
13.1.1 Network Controls.....	4
13.1.2 Security of Network Services	4
13.1.3 Segregation in Networks.....	5
13.2 Information Transfer.....	5
13.2.1 Information Transfer Procedures	5
13.2.2 Agreements on Information Transfer	5
13.2.3 Electronic Messaging	5
13.2.4 Confidentiality or Non-disclosure Agreements.....	6

13.0 Communications Security Policy

13.0.1 Purpose

13.0.1.1 The purpose of the RXO, Inc. (RXO) Communications Security Policy is to provide information security requirements for the processes related to network security management and information transfer. This document addresses network controls, security of network services and segregation in the network processes within the RXO. Additionally, the policy addresses information transfer procedures, agreements on information transfer, electronic messaging, and confidentiality or non-disclosure agreements.

13.0.2 Scope

13.0.2.1 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.

13.0.2.2 This policy applies to all RXO information, electronic and print.

13.1 Network Security Management

13.1.1 Network Controls

13.1.1.1 Networks must be managed, controlled and optimized to protect information in systems and applications and must include established responsibilities and procedures for managing all networking subsystems.

13.1.1.2 Where and whenever possible, operational responsibility for networks must be separate from computer operations.

13.1.1.3 All access to networks must be controlled. Authentication must be enabled through robust mechanisms/means that will prevent unintended access, e.g., physical access to internal networks, or username and password identification. Unused or unmonitored network segments and ports must be disabled.

13.1.2 Security of Network Services

13.1.2.1 Security mechanisms, service levels, and management requirements of all network services must be identified, monitored, subject to audit and included in network service agreements, whether these services are provided in-house or outsourced.

13.1.2.2 The security arrangements necessary for particular services (such as security features, service levels, and management requirements) must be formally documented.

13.1.3 Segregation in Networks

13.1.3.1 Groups of information services, users, and information systems must be segregated on networks, have limits on their access according to roles and responsibilities and restrict access by division into separate network domains through the use of physical or logical segmentation.

13.1.3.2 The domains must be established based on trust levels (e.g., public access domain, desktop domain, and server domain), organizational structures and units (e.g., human resources, finance, marketing) or some combination (e.g., server domain connecting to multiple organizational units).

13.1.3.2.A The perimeter of each domain must be delineated using well-defined criteria. The criteria for segregation of networks into domains, and the access allowed through the gateways, must be based upon domain-specific assessments of the security requirements.

13.1.3.3 Wireless networks require additional consideration due to the difficulties in controlling access to emitted media network perimeters. For the environments that are defined as sensitive, all wireless access must be segregated by approved electronic and/or physical methods, from the other internal networks. Access to these internal network segments must be validated through the use of approved gateways or other access control mechanisms.

13.1.3.4 Periodic (annual) risk assessments must be performed to determine where upgrades are needed based upon the system criticality, sensitivity of affected information and cost / benefit analysis.

13.2 Information Transfer

13.2.1 Information Transfer Procedures

13.2.1.1 Formal transfer procedures and controls must be in place to protect the transfer of information through the use of all types of communication facilities. In addition, training content must be provided for employees and contractors on topics relating to disclosure of confidential or sensitive information. Training content should include cautions on open conversations in public places or communications over insecure channels.

13.2.2 Agreements on Information Transfer

13.2.2.1 Agreements must address the secure transfer of business information between RXO and external parties and the content of any agreement must reflect the sensitivity of the business information involved.

13.2.3 Electronic Messaging

13.2.3.1 Information involved in electronic messaging must be appropriately protected and must address equivalent safeguards as those required for all other information transfers.

13.2.3.2 For electronic messaging involving sensitive or classified information, secure messaging protocols (e.g., end-to-end encryption) must be used to protect message integrity and confidentiality.

13.2.4 Confidentiality or Non-disclosure Agreements

13.2.4.1 Requirements for confidentiality or non-disclosure agreements reflecting RXO's needs for the protection of information must be identified, regularly reviewed, and documented.

13.2.4.1.A Confidentiality or non-disclosure agreements are applicable to all users accessing RXO information assets and must address requirements to protect confidential information using legally enforceable terms.

13.2.4.1.B Confidentiality and non-disclosure agreements must comply with all applicable laws and regulations for the jurisdiction(s) to which they are applicable.

13.2.4.1.C Confidentiality and non-disclosure agreements must be periodically reviewed to ensure continued applicability.

Certificate of Review

Communications Security Policy

December 18th 2025 10:22:28 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 3:15 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 10:58 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:22 AM EST