



Organization of Information Security Policy

DOC-IT-IS-O6
Revision 2.0
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	11/01/2025	RXO, Inc. updates, annual review

Table of Contents

6.0 Organization of Information Security Policy	4
6.0.1 Purpose	4
6.0.2 Scope	4
6.1 Internal Organization.....	4
6.1.1 Information Security Roles and Responsibilities	4
6.1.2 Segregation of Duties	4
6.1.3 Contact with Authorities	5
6.1.4 Contact with Special Interest Groups.....	5
6.1.5 Information Security in Project Management	5
6.2 Mobile Devices and Teleworking.....	6
6.2.1 Mobile Device Policy.....	6
6.2.2 Teleworking / Remote Working	6

6.0 Organization of Information Security Policy

6.0.1 Purpose

The purpose of the RXO, Inc. (RXO) Vulnerability Management Standard is to provide information security requirements for the processes related to management of security vulnerabilities within RXO systems and applications.

6.0.2 Scope

This Policy applies to:

- All of RXO, Inc., including all subsidiaries, divisions, and operating entities. All directors, officers, employees, contractors, and third parties acting on behalf of RXO must comply with this policy.
- This policy applies to all RXO entities, employees, agents, contractors, and third-party partners, as well as all data and systems used by or supporting the company.
- This policy applies to all information and other classes of protected information.

6.1 Internal Organization

6.1.1 Information Security Roles and Responsibilities

6.1.1.1 All information security responsibilities must be defined, documented, communicated and allocated.

6.1.1.1.A Information security responsibilities must include the responsibilities for the protection of individual assets and for carrying out specific information security processes based upon assigned roles, as well as responsibilities for information security risk management activities and, in particular, for acceptance of residual risks. Supplemental guidance for specific sites and information processing facilities, as well as local procedures, roles, and responsibilities for the protection of assets and execution of security processes specific to these areas, must be made available as needed.

6.1.1.1.B Information security roles and responsibilities must clearly describe the affected assets and information security processes, areas of responsibilities, details regarding supporting authorization levels and, where necessary, details regarding the required information security coordination and oversight with suppliers.

6.1.1.1.C Individuals may delegate allocated information security tasks to others if approved by the appropriate manager(s). Regardless of delegation, however, accountability for the successful task execution remains with the originally assigned individual(s).

6.1.2 Segregation of Duties

6.1.2.1 Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets. Conflicting duties and areas of responsibility must be segregated.

6.1.2.1.A User duties and responsibilities must be assigned so that no single role or user is able to access, modify, or use the assets without authorization or detection. Based upon the principles

of Least Privilege and need-to-know, user and role permissions must be defined following analysis from multiples aspects, including application-to-application, application-to-end-user computing and all inputs and outputs.

6.1.2.1.B Where difficulties exist in properly executing segregation of duties, the principle must be applied as far as is possible and practicable, and other compensating controls should be considered, e.g., enhanced auditing/monitoring of activities and management supervision.

6.1.3 Contact with Authorities

6.1.3.1 Appropriate contacts with relevant authorities must be maintained.

6.1.3.1.A The Chief Compliance Officer and SVP of Litigation will specify when law enforcement and/or regulatory bodies are to be contacted and how identified information security incidents are to be reported in a timely manner (e.g., if it is suspected that laws are broken).

6.1.3.1.B The practices must align with approved RXO security incident response, and business continuity roles, responsibilities, and activities.

6.1.4 Contact with Special Interest Groups

6.1.4.1 Appropriate contacts with special interest groups or other specialist security forums and professional associations must be maintained.

6.1.4.1.A Information on the RXO personnel memberships in special interest groups, other specialist security forums, and professional associations must be maintained and made easily accessible. The membership lists should be used for annual budgeting projection for maintaining the memberships.

6.1.4.1.B All individuals with information security responsibilities, whether assigned or inferred, should be encouraged to solicit membership in these special interest groups and forums to improve knowledge about best practices, to stay current with relevant security information developments and to maintain a complete understanding of the information security environment.

6.1.4.1.C Information sharing agreements can be established to improve cooperation and coordination of security issues. Such agreements should identify requirements for the protection of confidential information.

6.1.5 Information Security in Project Management

6.1.5.1 Information security must be addressed within project management, regardless of the type of the project.

6.1.5.1.A Information security must be incorporated within all phases of the project management methodology to ensure that information security risks are identified and remediated as part of any formal project or engagement. This applies to any project regardless of its character unless formally identified as an exception.

6.1.5.1.B Project objectives must include information security objectives, and an information security risk assessment must be conducted at an early stage in a project to identify any required remediation. All required remediation actions must be reviewed and approved by Information Security personnel as having been successfully completed prior to implementation.

6.1.5.1.C Responsibilities for information security must be defined and allocated to specified roles in the project management methodology.

6.2 Mobile Devices and Teleworking

6.2.1 Mobile Device Policy

6.2.1.1 Standards and supporting security measures must be adopted to manage the risks introduced by using mobile devices.

6.2.1.1.1 Implement appropriate standards to control the risks of working with mobile devices, and to ensure that business information is not compromised through the use of mobile devices. Additional protective measures must be established to address working with mobile devices in unprotected environment(s).

6.2.1.1.2 The use of privately-owned mobile devices are allowed upon satisfaction of relevant mobile device entrance criteria based on industry best practices. All mobile devices must ensure separation of private and business use of the devices, including using software to support such separation and protect business data on a private device.

6.2.1.1.3 All users of privately owned mobile devices must sign an end user agreement acknowledging their duties (e.g., physical protection, software updating, etc.), waiving ownership of business data and allowing remote wiping of data, excluding personal data, by RXO in case of theft or loss of the device or when no longer authorized to use the service based on industry best practices.

6.2.1.1.4 All users receiving or using mobile devices that may be used to store, transmit or process sensitive information must be provided additional information security training to raise awareness of the risks incurred through the use of using mobile devices. At a minimum, this training must be delivered at the time of mobile device issuance or configuration.

6.2.1.1.5 In the event of known or suspected theft or loss of a mobile device containing sensitive information, the user must immediately notify the Help Desk.

6.2.1.1.6 After the device has been determined to be lost or stolen (and not misplaced), the Help Desk should immediately wipe the device.

6.2.2 Teleworking / Remote Working

6.2.1.2 Security measures must be implemented to protect company-owned equipment and information accessed, processed, or stored at teleworking/remote working sites.

6.2.1.2.1 Processes must be implemented to define the conditions and restrictions for utilizing teleworking/remote working arrangements and address the accessing, processing, and storing of information at the teleworking/remote working sites.

6.2.1.2.2 All teleworking/remote working arrangement conditions must conform to pertinent security requirements. These requirements must be communicated to end users prior to any teleworking/remote working activities and subjected to annual risk assessments.

6.2.1.2.3 All remote access originating outside the trusted RXO internal network, and other identified remote access applications which RXO management deems necessary, must require the use of multi-factor authentication for both end-user and administrative access to the internal network and resources.

Certificate of Review

Organization of Information Security Policy

December 18th 2025 11:02:03 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 2:00 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:27 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 11:02 AM EST