



Information Security Policy

DOC-IT-IS-O5
Revision 2.1
NOVEMBER 1, 2025

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

5.0 Information Security Policy	4
5.0.1 Purpose	4
5.0.2 Scope.....	4
5.1 Information Security Roles and Responsibilities.....	4
5.2 Segregation of Duties	4
5.3 Management Direction for Information Security.....	5
5.3.1 Policies for Information Security.....	5
5.3.2 Review and Update of the Policies for Information Security.....	6
5.4 Enforcement.....	6
5.4.1 Violations	6
5.4.2 Policy Exceptions and Variances Process.....	6

5.0 Information Security Policy

5.0.1 Purpose

5.0.1.1 The purpose of the RXO, Inc. (RXO) Information Security Policy is to outline the responsibilities and expectations for security of information assets managed by RXO. The controls described in this policy are collectively known as RXO's Security Program, which is designed to reflect RXO's business objectives, prevent the unauthorized use of or access to our information systems and maintain the confidentiality, integrity, and availability of information assets.

5.0.1.2 This policy is guided by security requirements specific to the RXO operating environment, laws, and regulations that are relevant to RXO and information security best practices. These control requirements are documented and aligned with an internationally recognized industry standard for security, ISO 27002, *Code of Practice for Information Security Management*.

5.0.2 Scope

5.0.2.1 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.

5.0.2.2 The policy applies to all classes of protected information.

5.1 Information Security Roles and Responsibilities

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

5.1.1.1.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 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.

5.1.1.1.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.

5.1.1.1.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).

5.2 Segregation of Duties

5.2.1.1 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.

5.2.1.1.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.

5.2.1.1.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.

5.3 Management Direction for Information Security

5.3.1 Policies for Information Security

5.3.1.1 A set of policies for information security must be defined, approved by management, published, and communicated to employees and relevant external parties.

5.3.1.1.A At the highest level, RXO's Board of Directors has empowered senior management with the responsibility and requirement to apply due diligence in all aspects concerning information security. To support this obligation, the internal controls and objectives are established and embodied in an "information security policy" framework. The framework has been approved by management and specifies the designated approach for managing RXO's information security objectives.

5.3.1.1.B The information security policy framework addresses requirements in accordance with business strategy, regulations, legislation and contracts and the current and projected information security threat environment. These obligations are subject to periodic (annual) consideration as part of the annual policy review and update cycle.

5.3.1.1.C Senior management must implement an information security, internal controls framework that protects all sensitive data, applications, assets, and clients. This framework must be fully defined through a collection of sub-policies that support the overall information security approach and framework.

5.3.1.1.D Senior management must ensure these policies are communicated to employees and relevant external parties in a form that is relevant, accessible, and understandable to the intended reader (e.g., in the context of an "information security awareness, education and training program").

5.3.2 Review and Update of the Policies for Information Security

5.3.2.1 The policies for information security must be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

5.3.2.1.A Each policy must have an owner who has approved management responsibility for the development, review, and evaluation of their assigned governance documentation. The review must include assessing opportunities for improvement of the policies and approach to managing information security in response to changes to the environment, business circumstances, legal conditions, or technical environment.

5.3.2.1.B The review of policies for information security must consider the results of periodic (annual) evaluations of the content by management. The remediation strategy must be specific; each item must have an owner, and the item must have a completion date.

5.3.2.1.C Requests for revision to a policy must receive management approval before the revised policy is effective. All revisions to policies must document the specific change and follow a documentation version control process.

5.4 Enforcement

5.4.1 Violations

5.4.1.1 Users detecting violations of any RXO policy must immediately report the violation to their direct manager, who must verify the nature of the violation and report it to the RXO Global Security Office. A determination must be made by the RXO Global Security Office as to the extent of risk that any non-compliance condition presents and what remediation activities are required. Examples of violations may include sharing passwords, accessing systems without proper authorization, failure to report a lost device containing RXO data, or downloading unauthorized software that may compromise RXO's security environment.

5.4.1.2 Users who deliberately violate information security policies will be subject to disciplinary action up to and including termination of employment or association with RXO.

5.4.2 Policy Exceptions and Variances Process

5.4.2.1 In the event that current practices or business needs require that exceptions or variances be made to any RXO policy, a formal exception/variance must be obtained, using the RXO Policy Exception/Variance Process provided herein in this policy. For all intents and purposes, this section defines the full set of controls for the Policy Exceptions and Variances Process.

This process requires documenting the details of the circumstances and the details of the business case for the needed control circumvention and/or compensating controls. It also requires obtaining approval from senior management as well as the RXO Global Security Office.

5.4.2.2 The approved exceptions must be reviewed on a quarterly basis to ensure that the risks associated with the exceptions remain at acceptable levels. Where the risks have changed to a significant degree, the previously granted exceptions may be revoked by the RXO Global Security Office.

Certificate of Review

Information Security Policy

December 18th 2025 11:01:27 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Monday, November 24, 2025 10:12 AM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:27 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 11:01 AM EST