



Human Resources IT Security Policy

DOC-IT-IS-07
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

7.0 Information Security Policy	4
7.0.1 Purpose	4
7.0.2 Scope	4
7.1 Prior to Employment	4
7.1.1 Screening	4
7.1.2 Terms and Conditions of Employment	5
7.2 During Employment	5
7.2.1 Management Responsibilities.....	5
7.2.2 Information Security Awareness, Education and Training.....	5
7.2.3 Disciplinary Process	6
7.3 Termination and Change of Employment	6
7.3.1 Termination or Change of Employment Responsibilities.....	6

7.0 Information Security Policy

7.0.1 Purpose

7.0.1.1 The purpose of the RXO Human Resources Security Policy is to ensure that information security measures are applied consistently throughout the employment life cycle. This policy aims to mitigate insider threats, secure access to sensitive data, and ensure compliance with data protection regulations before, during, and after employment.

7.0.2 Scope

7.0.2.1 This policy applies to all RXO subsidiaries, divisions, and operating entities, all employees, potential employees, agents, and contractors, as well as all data and information systems used by or supporting the company.

7.0.2.2 This policy encompasses all phases of the employment life cycle.

7.0.2.3 This policy applies to all sensitive information and other classes of protected information.

7.1 Prior to Employment

7.1.1 Screening

7.1.1.1 Background verification checks on all candidates for employment must be carried out in accordance with relevant laws, regulations, and ethics and must be proportional to the business requirements, the classification of the information to be accessed and the perceived risks, taking into account relevant statutes, protection of PII and employment-based legislation.

7.1.1.1.A When an individual is hired for a sensitive role, the company must make sure the candidate has the necessary competence to perform the assigned security role, and that the individual can be trusted to take on the role, especially if the role is deemed critical or has access to sensitive data and systems.

7.1.1.1.B Additional verification must be performed on either initial appointments or promotions when the new position involves access to information processing facilities. These more rigorous verification activities are especially important if the new position requires regular access to confidential information, e.g., financial information, sensitive information, or regulated information.

7.1.1.1.C The screening process must also address the onboarding of contractors. Notification procedures need to be followed if screening has not been completed or if the results give cause for doubt or concern.

7.1.1.1.D All applicant information must be collected and handled in accordance with all appropriate legislation existing in the relevant jurisdiction. Candidates must be informed beforehand about the screening activities.

7.1.2 Terms and Conditions of Employment

7.1.2.1 The contractual agreements with employees and contractors must state their and RXO's responsibilities for information security.

7.1.2.1.A The contractual agreements with users must state all responsibilities for information security.

7.1.2.1.B The contractual obligations for users must reflect RXO's policies for information security.

7.1.2.1.C Information security roles and responsibilities must be communicated to job candidates during the pre-employment process.

7.1.2.1.D All users must agree to the terms and conditions governing their information security responsibilities appropriate to the nature and extent of user access.

7.1.2.1.E Responsibilities contained within the terms and conditions of employment must continue for a defined period after the end of the employment, where appropriate.

7.2 During Employment

7.2.1 Management Responsibilities

7.2.1.1 Management must require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

7.2.1.1.A All users must be properly briefed to perform their information security roles and responsibilities prior to being granted access to confidential information or information systems. All users must receive sufficient periodic training to achieve a level of awareness on information security relevant to their roles and responsibilities within RXO. Users must also conform to the terms and conditions of employment, including RXO's information security policies.

7.2.1.1.B All users must have access to anonymous reporting channels to report violations of information security policies or procedures ("whistle blowing").

7.2.1.1.C Management must demonstrate support of information security policies, procedures, and controls.

7.2.2 Information Security Awareness, Education and Training

7.2.2.1 All employees and contractors must receive appropriate awareness education and training, and regular updates in organizational policies and procedures, as relevant for their job function.

7.2.2.1.A An information security awareness program must be in place to ensure that all users receive appropriate information security education and awareness training, as relevant for their job function. Information security awareness education and training must take place at hire and thereafter at least annually and must be provided to both new hires and users who transfer to new positions or roles with substantially different information security requirements. Managers are responsible for ensuring employees complete assigned training. User accounts or privileges may be suspended until mandatory security awareness training is completed.

7.2.2.1.B The information security awareness program must be established in line with RXO's information security policies and relevant procedures, taking into consideration the information to be protected and the controls that have been implemented to protect the information.

7.2.2.1.C The information security awareness program must consider employees' roles in the company, and, where relevant, the expectations for contractors. The program must also be updated regularly so that it stays in line with RXO policies and procedures and must be built upon lessons learned from information security incidents.

7.2.2.1.D The information security awareness program must provide users with awareness of their responsibilities for information security and the means by which those responsibilities are discharged.

7.2.3 Disciplinary Process

7.2.3.1 There must be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach or other violation of RXO security policies.

7.2.3.1.A A formal disciplinary process must be established in order to take action against users who have committed an information security breach. This disciplinary process should not be initiated without prior verification that an information security event has occurred.

7.2.3.1.B The disciplinary process must ensure correct and fair treatment for users who are suspected of committing breaches of information security policy. The process must provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach, and its impact on business, whether or not this is a first or repeat offense, whether or not the violator was properly trained, relevant legislation, business contracts, and other factors, as appropriate.

7.2.3.1.C The disciplinary process should also be used as a deterrent to prevent users from violating RXO's information security policies and procedures and any other information security breaches.

7.3 Termination and Change of Employment

7.3.1 Termination or Change of Employment Responsibilities

7.3.1.1 Information security responsibilities and duties that remain valid after termination or change of employment must be defined, communicated to the employee or contractor, and enforced.

7.3.1.1.A An Information security responsibilities and duties that remain valid after termination or change of employment must be defined, communicated to the user, and enforced by management. Responsibilities and duties still valid after termination of employment must be contained in the user's terms and conditions of employment. RXO shall keep records of staff involuntarily terminated and shall not re-hire such individuals without Human Resources' approval.

7.3.1.1.B The communication of termination responsibilities must include on-going information security requirements and legal responsibilities. Where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment may continue

for a defined period after the end of the user's employment and should also be communicated to the departing individual.

7.3.1.1.C Changes of responsibility or employment must be managed as defined in the Access Management Policy, ensuring that users are provided only the needed levels of access according to their responsibilities.

Certificate of Review

Human Resources IT Security Policy

December 18th 2025 11:02:53 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Monday, November 24, 2025 12:13 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