



Asset Management Policy

DOC-IT-IS-O8
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 and annual review

8.0 Asset Management Policy	4
8.0.1 Purpose	4
8.0.2 Scope	4
8.1 Responsibility for Assets	4
8.1.1 Inventory of Assets	4
8.1.2 Ownership of Assets	4
8.1.3 Acceptable Use of Assets	4
8.1.4 Return of Assets	5
8.2 Information Classification	5
8.2.1 Classification of Information	5
8.2.2 Labelling of Information	6
8.2.3 Handling of Assets	6
8.3 Media Handling	6
8.3.1 Management of Removable Media	6
8.3.2 Disposal of Media	6
8.3.3 Physical Media Transfer	7

8.0 Asset Management Policy

8.0.1 Purpose

8.0.1.1 The purpose of the RXO Asset Management Policy is to provide information security requirements regarding the management of assets and the handling of physical and electronic media at RXO. Inappropriate use exposes RXO to risks, including compromise of network systems and services, human resources or legal issues.

8.0.2 Scope

8.0.2.1 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.

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

8.1 Responsibility for Assets

8.1.1 Inventory of Assets

8.1.1.1 Assets associated with information processing facilities and information storage, or processing must be identified and an inventory of these assets shall be drawn up and maintained.

8.1.1.2 The asset inventory must be accurate, up to date, and consistently aligned with other inventories.

8.1.1.3 For each of the identified assets, ownership of the assets must be assigned (see 8.1.2), and appropriate classification level(s) must be identified (see 8.2).

8.1.2 Ownership of Assets

8.1.2.1 Assets maintained in the inventory must be owned.

8.1.2.1.A Asset ownership must be assigned to an individual or group. The asset owner will be responsible for lifecycle management of applicable elements by tracking; when the asset is introduced to or migrated within the organization.

8.1.2.1.B The asset owner is responsible for the proper oversight, including ensuring that assets are inventoried; verification that assets are appropriately classified and protected; definition and periodic review of access restrictions and classifications of critical operational assets, taking into account applicable access control policies; and ensuring proper handling when the asset is deleted or destroyed.

8.1.3 Acceptable Use of Assets

8.1.3.1 Rules for the acceptable use of information and of assets associated with information and information processing facilities must be identified, documented, and implemented.

- 8.1.3.1.A** All users with access to the company's assets must be made aware of the information security requirements of the company's assets associated with information and information processing facilities and resources. Users must understand that they are responsible for all activities performed with assigned access to and use of these information processing resources.

8.1.4 Return of Assets

8.1.4.1 All employees and external party users must return all of the organizational assets in their possession upon termination of their employment, contract, or agreement.

- 8.1.4.1.A** In cases, where an employee or external party user purchases the company's equipment or uses their own personal equipment, procedures must specify that all relevant information is to be transferred to the company and is to be securely erased from the equipment. This erasure must occur by using RXO approved tools to securely wipe the contents of the drives or removable media, or by physically destroying the media.

- 8.1.4.1.B** Where an employee or external party user has knowledge of or access to information that is deemed critical to ongoing operations, this knowledge and/or access must be documented and transferred to RXO. During the termination notification period, data owners and employee managers must control all unauthorized copying of relevant information (e.g., intellectual property) by terminated employees and contractors.

8.2 Information Classification

8.2.1 Classification of Information

8.2.1.1 Information must be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorized, disclosure or modification.

- 8.2.1.1.A** Information assets must be classified and labeled according to existing classification standards. The associated protective controls must take into account any business needs for sharing or restricting information, as well as legal requirements.
- 8.2.1.1.B** Classification of assets other than information must conform to the most sensitive level of classification of the information which it is stored in, processed by, handled with, or protected by the asset.
- 8.2.1.1.C** Owners of information assets are accountable to ensure that the assets are protected based on their classification.
- 8.2.1.1.D** The classification scheme must include conventions for categorizing information and the criteria for reviewing these values over time. The level of protection in the scheme must be assessed by analyzing confidentiality, integrity, availability, possession, authenticity and utility and any other requirements for the information considered. The name of each level of categorization must convey a name that makes sense in the context of the classification scheme's application. The classification scheme should be aligned to access control practices.

8.2.1.1.E The classification scheme should be incorporated into RXO processes and must be consistent and coherent across the organization to ensure that all classification activities are performed equivalently and that all users have a common understanding of protection requirements.

8.2.1.1.F Classifications assigned to specific assets should be reviewed and updated in accordance with changes to their value, sensitivity, and criticality throughout their life cycle.

8.2.2 Labelling of Information

8.2.2.1 An appropriate set of labeling procedures for information labelling must be implemented in accordance with the information classification scheme adopted by RXO and clearly reflect the classification standard.

8.2.2.1.A The labeling procedures must provide guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled, depending on the types of media.

8.2.2.1.B The labeling procedures must define cases where labeling is omitted, e.g., labeling of nonconfidential information to reduce workloads.

8.2.2.1.C Output from systems containing information assets that are classified as must carry an appropriate classification label.

8.2.3 Handling of Assets

8.2.3.1 Procedures for asset handling, processing, storing, and communicating must be implemented in accordance with the information classification scheme adopted by RXO.

8.2.3.1.A Agreements with other organizations that include information sharing must include procedures to identify the classification of that information and to interpret the classification labels from other organizations.

8.3 Media Handling

8.3.1 Management of Removable Media

8.3.1.1 Procedures must be implemented for the management of removable media in accordance with the classification scheme adopted by RXO.

8.3.1.1.A Procedures and authorization levels must be documented.

8.3.2 Disposal of Media

8.3.2.1 Media must be securely disposed of when no longer required, using formal procedures.

8.3.2.1.A Media containing confidential information must be stored and disposed of securely. Procedures must be in place to identify the items that might require secure disposal. Where necessary, third-party organizations may be used to collect and dispose of media.

8.3.2.1.B Disposal of sensitive items must be logged in order to maintain audit trails.

8.3.3 Physical Media Transfer

8.3.3.1 Media containing information must be protected against unauthorized access, misuse, or corruption during transportation.

8.3.3.1.A RXO must establish and implement secure procedures for the transfer of physical media containing information. These procedures should address the use of reliable transport services, safeguarding the content during transit, and maintaining sufficient logging to track the media's movement.

Certificate of Review

Asset Management Policy

December 18th 2025 11:03:26 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 2:29 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:28 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 11:03 AM EST