



Terms and Definition Standard

DOC-IT-IS-22
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. Revisions, annual review

Table of Contents

22.0 Terms and Definitions Standard4

22.0.1 Purpose4

22.0.2 Scope4

22.0.3 Policies for Information Security4

22.0 Terms and Definitions Standard

22.0.1 Purpose

22.0.1.1 The purpose of the RXO, Inc. including its subsidiaries, divisions and any other operating entities (collectively, "RXO") Terms and Definition Standard is to provide a repository that details the meaning and intent of the various topics and abbreviations used through the RXO policy and standards documents.

22.0.2 Scope

22.0.2.1 This standard applies to all RXO security governance documents.

22.0.3 Policies for Information Security

Access Control – Means to ensure that access to assets is authorized and restricted based on business and security requirements.

Accountability – Responsibility of an entity for its actions and decisions.

Alternate Storage – Any storage location other than Protected Storage, such as but not limited to a local workstation disk or a flash drive.

Asset – Anything that has value to the organization. There are many types of assets, including information; software, such as a computer program; physical, such as computers; services; people, and their qualifications, skills, and experience; and intangibles, such as reputation and image.

Authenticity – Property that an entity is what it claims to be.

Availability – Property of being accessible and usable upon demand by an authorized entity. Business Continuity – Processes and/or procedures for ensuring continued business operations.

Business Impact Analysis (BIA) – Process used to identify which business units/departments and processes are essential to the survival of RXO as part of the business continuance program's prioritization and execution.

Confidentiality – Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Confidential Information – Business and technical information used in RXO business (all or any portion of which, and the materials on which they are used, whether or not specifically labeled or identified as "confidential" or "proprietary" whether or not created by the Internal User or other RXO employees or agents or committed to the Internal User's memory, in any form or medium – tangible or intangible), including, but not limited to, information concerning formulas, raw materials, techniques, product assembly, production processes, production statistics, equipment design, repair sequences, geographic locations of proposed facilities, packaging, distribution, capacity, systems, specifications, financial information (budgets, forecasting, projections, pricing, including pricing models, government bid information, and costs), employee information (payroll and benefits information, training programs and personnel records), marketing plans and proposals and customer presentations including graphics, facility photos and data, customer "case studies", "client volumes", client/customer Statements of Work ("SOW"), inventions, trade secrets, patents, copyrights and trademarks, manufacturing, inventory, products, shipping, computer information (programs, databases, information technology, architecture, hardware and software), contractual agreements, information subject to mutual nondisclosure agreements, and Customer Information, or any information not otherwise available in the public domain.

Control – Means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be administrative, technical, management, or legal in nature. Control is also used as a synonym for safeguard or countermeasure.

Control Objective – Statement describing what is to be achieved because of implementing controls.

Corrective Action – Action to eliminate the cause of a detected nonconformity or other undesirable situation.

Critical Data – Includes any types of data that are defined by RXO as being critical data that must be protected and controlled to maintain RXO operations.

Customer Information – Information provided by a customer including but not limited to, order data or customer e- mail messages. Customer contracts may specify Customer-specific classification or information handling requirements.

Data Owner – RXO employee with responsibility for specific RXOIS who is authorized to give management approval for access to RXOIS and to determine data classification. The Data Owner is typically a non-RXO employee.

Effectiveness – Extent to which planned activities are realized and planned results achieved. Efficiency – Relationship between the results achieved and how well the resources have been used.

Event – Occurrence of a particular set of circumstances.

External User(s) – Anyone who is authorized by RXO to use or to access RXOIS, other than Internal Users. External Users include, but are not limited to clients, customers, business partners, vendors, and their respective employees, and any other third party to whom RXO has provided access to RXOIS.

GDPR Personal Data – Any information relating to an identified or identifiable natural person ('data subject') who is a citizen of the EU; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

GDPR Special Categories of Personal Data – Any personal data related to a citizen of the EU, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. This data is prohibited from being processed with specific exception defined in GDPR Article 9, paragraph 2 (a) through 2 (j).

Guideline – Recommendation of what is expected to be done to achieve an objective.

Impact – Adverse change to the level of business objectives achieved.

Information Asset – Knowledge or data that has value to the organization.

Information Security – Preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, nonrepudiation, and reliability can also be involved.

Information Security Event – Identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.

Information Security Incident – Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Information Security Incident Management – Processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Information Security Management System (ISMS) – Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.

Information Security Risk – Potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization.

Integrity – Property of protecting the accuracy and completeness of assets.

Internal User(s) – Any and all users of RXOIS, individually or collectively, who are temporary, part-time, or regular full-time employees, contractors, subcontractors, consultants, and other workers for RXO.

Malware – Malicious software including viruses, worms, spyware, keystroke loggers, and a wide variety of other software used to corrupt data, damage systems, collect information, or disrupt activities.

Management System – Framework of policies, procedures, guidelines, and associated resources to achieve the objectives of the organization.

Nonrepudiation – Ability to prove the occurrence of a claimed event or action and its originating entities, in order to resolve disputes about the occurrence or nonoccurrence of the event or action and involvement of entities in the event.

Policy – Overall intention and direction as formally expressed by management.

Preventive Action – Action to eliminate the cause of a potential nonconformity or other undesirable potential situation.

Procedure – Specified way to carry out an activity or a process.

Process – Set of interrelated or interacting activities which transform inputs into outputs.

Profane Material – Material that is offensive, sexually explicit, profane, pornographic, harassing, or intimidating, including that which violates 18 U.S.C. § 223 or other federal or state sexual harassment or hostile workplace laws or regulations.

Protected Storage – An authorized data storage device for RXOIS, typically a specified location on an RXO device, managed and regularly backed up by the Global Security Office.

Record – Document stating results achieved or providing evidence of activities performed. Reliability – Property of consistent intended behavior and results.

Risk – Combination of the probability of an event and its consequence.

Risk Acceptance – Decision to accept a risk.

Risk Analysis – Systematic use of information to identify sources and to estimate risk. Risk analysis provides a basis for risk evaluation, risk treatment, and risk acceptance.

Risk Assessment – Overall process of risk analysis and risk evaluation.

Risk Communication – Exchange or sharing of information about risk between the decision maker and other stakeholders.

Risk Criteria – Terms of reference by which the significance of risk is assessed.

Risk Estimation – Activity to assign values to the probability and consequences of a risk.

Risk Evaluation – Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

Risk Management – Coordinated activities to direct and control an organization regarding risk. Risk management generally includes risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring, and risk review.

Risk Treatment – Process of selection and implementation of measures to modify risk.

Sensitive Data – Includes U.S. Personally Identifiable Information (PII) data, U.S. HIPAA data, GDPR Personal Data, intellectual property data, and any other RXO defined sensitive data.

Statement of Applicability – Documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS.

Threat – Potential cause of an unwanted incident, which may result in harm to a system or organization.

User – All personnel, whether employees, agents, contractors, or third-party service providers, who access RXO information assets.

Utility – The usefulness of information.

Variance – Exemption from a security policy or standard when the requirements for a control cannot be satisfied for business or technical reasons.

Vulnerability – Weakness of an asset or control that can be exploited

by a threat. RXO – RXO, Inc., its subsidiaries, divisions and any other operating entities.

RXO Information Systems (RXOIS) – All RXO owned, operated, or provided information technology-related hardware, software, equipment, facilities, information, and services, including but not limited to:

RXO Senior Management – For purposes of this Policy, RXO personnel who hold Vice President level positions or higher.

RXO Sponsoring Manager – A designated Internal User who is responsible for managing an Internal User or External User's access to RXOIS. The RXO Sponsoring Manager is typically an RXO employee.

RXO Global Security Office – RXO employees who are primarily responsible for the maintenance, operation, or security of RXOIS.

Certificate of Review

Terms and Definitions Standard

December 18th 2025 10:36:38 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 4:02 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:14 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:36 AM EST