



Systems Acquisition, Development, and Maintenance Policy

DOC-IT-IS-14
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 Revision
2.1	11/01/2025	RXO, Inc updates, annual review

Table of Contents

14.0 Systems Acquisition, Development and Maintenance Policy	4
14.0.1 Purpose	4
14.0.2 Scope	4
14.1 Security Requirements of Information Systems	4
14.1.1 Information Security Requirements Analysis and Specification	4
14.1.2 Securing Application Services on Public Networks	4
14.1.3 Protecting Application Services Transactions	5
14.2 Security in Development and Support Processes	5
14.2.1 Secure Development Policy	5
14.2.2 System Change Control Procedures	6
14.2.3 Technical Review of Applications after Operating Platform Changes	6
14.2.4 Restrictions on Changes to Software Packages	6
14.2.5 Secure System Engineering Principles	7
14.2.6 Secure Development Environment	7
14.2.7 Outsourced Development	7
14.2.8 System Security Testing	7
14.2.9 System Acceptance Testing	8
14.3 Test Data	8
14.3.1 Protection of Test Data	8

14.0 Systems Acquisition, Development and Maintenance Policy

14.0.1 Purpose

14.0.1.1 The purpose of the RXO, Inc. (RXO) Systems Acquisition, Development, and Maintenance Policy is to provide information security requirements for the processes related to performing system acquisition, development, and maintenance activities for RXO systems and applications.

14.0.2 Scope

14.0.2.1 This policy applies to all RXO subsidiaries, divisions, and operating entities, all employees, agents, contractors, and third-party partners of RXO and its subsidiaries (including boutiques), as well as all data and systems used by or supporting the company.

14.0.2.2 This policy addresses information security requirements for the processes related to the security requirements of information systems, security in development and support, as well as test data.

14.0.2.3 This policy applies to all information and data owned or managed by RXO.

14.1 Security Requirements of Information Systems

14.1.1 Information Security Requirements Analysis and Specification

14.1.1.1 The information security related requirements must be included in the requirements for new information systems or enhancements to existing information systems and must reflect the business value of the information involved.

14.1.1.1.A Information security requirements, including legal, regulatory, contractual, and compliance obligations, must be identified for all systems development/enhancements, based on policies and regulations, threat modeling, incident reviews, use of vulnerability thresholds, etc. and formally documented and approved by the appropriate stakeholders.

14.1.1.1.B Security requirements for all system acquisitions and developments must follow a standardized security requirements template, ensuring consistency across projects and easier compliance verification.

14.1.1.1.C For all third-party solutions, associated contracts with the supplier must include the identification of security requirements. A formal testing and acquisition process must be established to ensure that information security requirements are fully met prior to acquisition. Where the security functionality in a proposed product does not satisfy the information security requirements, the risk introduced and associated controls must be reviewed, remediated, and/or accepted prior to purchasing the product.

14.1.2 Securing Application Services on Public Networks

14.1.2.1 Information involved in application services passing over public networks must be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

14.1.2.1.A Cryptographic controls must be applied as applicable to satisfy the above considerations, taking into account compliance and legal requirements.

14.1.2.1.B Application service arrangements between partners must be supported by a documented agreement which commits both parties to the agreed terms of services, including details of the authorization.

14.1.2.1.C Consideration of resilience requirements against attacks must include requirements for protecting the involved application servers or ensuring the availability of network interconnections required to deliver the service.

14.1.3 Protecting Application Services Transactions

14.1.3.1 Information involved in application service transactions must be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay.

14.1.3.2 Transaction security controls must include non-repudiation and integrity verification to prevent unauthorized access, replay, or duplication attacks.

14.2 Security in Development and Support Processes

14.2.1 Secure Development Policy

14.2.1.1 Rules for the development of software and systems must be established and applied to developments within the organization to ensure that secure development environment(s), including secure services, architecture, software and systems, are utilized.

14.2.1.1.A The rules must address secure development and support activities throughout the development lifecycle; approved software development methodologies and secure coding guidelines for each programming language used; secure repositories; effective version control; and required developer application security knowledge needed to avoid, find, and fix vulnerabilities. Rules must address support activities after the development lifecycle, such as maintaining the software ability to be secure from vulnerabilities.

14.2.1.1.B Secure programming techniques must be utilized for both new development and any re-use of code scenarios where the standards applied to development may not be known or consistent with current best practices. Secure coding standards should be considered and where relevant mandated for use.

14.2.1.1.C Developers must receive training in secure development and testing practices. Mandatory development process related code reviews (by management and peers) must be used to ensure the ongoing effectiveness and use of this training.

14.2.1.1.D If development is outsourced, assurance must be obtained (through both contractual language and provided evidence of adherence) that the external party complies with internally expected rules for secure development (see the RXO Systems Development Lifecycle Standards and the RXO Supplier Relationships Policy for more details)

14.2.2 System Change Control Procedures

14.2.2.1 Changes to systems within the development lifecycle must be controlled by the use of formal change control procedures.

14.2.2.1.A The change control process must involve a risk assessment to analyze the impacts of planned changes and identify any needed remediation to security control deficiencies. The process must ensure that existing security and control procedures are not compromised, that developers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

14.2.2.1.B Wherever practicable, application and operational change control procedures must have proper integration.

14.2.2.1.C Automated auditing tools must be used to log and monitor changes to production systems, with alerts for unauthorized changes

14.2.3 Technical Review of Applications after Operating Platform Changes

14.2.3.1 When operating platforms are changed, business critical applications must be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

14.2.3.1.A Changes to operating platforms and critical business applications requires an annual review of application control and integrity procedures to ensure that they have not been compromised by the operating platform changes.

14.2.3.1.B Any change to the operating platform must include an impact analysis covering potential security implications on applications, configurations, and dependencies

14.2.4 Restrictions on Changes to Software Packages

14.2.4.1 Modifications to software packages must be discouraged, limited to necessary changes and all changes must be strictly controlled.

14.2.4.1.A Where feasible, vendor-supplied software packages must be implemented without modification. Where a software package needs to be modified, the following factors must be considered: the risk of built-in controls and integrity processes being compromised; whether the consent of the vendor should be obtained; the possibility of obtaining the required changes from the vendor as standard program updates; the impact if RXO becomes responsible for the future maintenance of the software as a result of the changes; and compatibility with other software in use.

14.2.4.1.B If changes are necessary, the original software must be retained and modifications applied to a designated copy of the original software. A software update management process must be developed, documented, and implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software. All changes must be fully tested and documented to support reapplication, if necessary, to future software upgrades.

14.2.4.1.C If required, modifications should be tested and validated by an independent evaluation body.

14.2.5 Secure System Engineering Principles

14.2.5.1 Principles for engineering secure systems must be established, documented, maintained, and applied to any information system implementation efforts.

14.2.5.1.A Security must be included in the design of all architectural layers (business, data, applications, and technology), while balancing the need for information security with the need for accessibility. Evaluation of new technology must include all aspects of security risks and the design must be reviewed against known attack patterns.

14.2.5.1.B These principles and procedures must be periodically reviewed to ensure that they are effectively contributing to enhanced standards of security within the engineering process and that they remain up to date in terms of combating any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.

14.2.5.1.C The established security engineering principles must apply, where applicable, to outsourced information systems through the contracts and other binding agreements between RXO and the supplier(s) used for outsourced services and support. Regular reviews must be conducted to confirm that the rigor of external suppliers' security engineering principles is comparable to those used within RXO.

14.2.6 Secure Development Environment

14.2.6.1 The organization must establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

14.2.6.1.A A secure development environment must include governance of the people, processes, and technology associated with system development and integration.

14.2.6.1.B Risks associated with individual system development efforts must be assessed, and secure development environments must be established for specific system development efforts.

14.2.6.1.C Strict access controls, including multi-factor authentication (MFA), must be applied to secure development environments to prevent unauthorized access.

14.2.7 Outsourced Development

14.2.7.1 The organization must supervise and monitor the activity of outsourced system development.

14.2.7.2 Third-party development vendors must undergo regular security audits to confirm adherence to RXO's secure development requirements

14.2.8 System Security Testing

14.2.8.1 Testing of the security functionality must be carried out during development.

14.2.8.1.A New and updated systems must receive thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities, test inputs, and expected outputs under a range of conditions. For in-house developments, such tests must initially be performed by the development team. Independent acceptance testing must then be

undertaken (both for in-house and for outsourced developments) to ensure that the system and/or application functions within expected criteria.

14.2.8.1.B The extent of testing must be in proportion to the importance and nature of the system.

14.2.8.1.C Existing systems must be tested for security functionality even if there are no current enhancements to the system. The security testing processes, must include the preparation of a detailed schedule of activities, test inputs, and expected outputs under a range of conditions. The testing or existing systems should occur on a rotating basis to ensure that all existing systems are tested within an 18-month rolling timeframe. The extent of testing must be in proportion to the importance and nature of the system.

14.2.9 System Acceptance Testing

14.2.9.1 Acceptance testing programs and related criteria must be established for new information systems, upgrades, and new versions.

14.2.9.1.A System acceptance testing must include testing of information security requirements and adherence to approved secure system development practices (see the RXO Systems Development Lifecycle Standards for more details).

14.2.9.1.B Testing activities must cover the depth and breadth of the affected system(s) and application(s) and must include all received components and integrated systems. Automated tools, such as code analysis tools or vulnerability scanners, should be leveraged, and the remediation of security-related defects must be verified in accordance with common practices.

14.2.9.1.C Testing must occur in a realistic test environment to ensure reliable results and that the system will not introduce vulnerabilities into the environment.

14.3 Test Data

14.3.1 Protection of Test Data

14.3.1.1 Test data must be selected carefully, protected, and controlled.

14.3.1.1.A Fabricated data rather than live production data must be used for testing wherever possible and security controls must be applied to protect production data when it must be used for testing purposes. Data should be obfuscated at a minimum.

Certificate of Review

Systems Acquisition, Development and Maintenance Policy

December 18th 2025 10:26:33 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 4:15 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 10:59 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:26 AM EST