



Change Management Policy

DOC-IT-IS-37
Revision 1.0
MARCH 20, 2026

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 © 2026 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	03/20/2026	Initial Version

Table of Contents

35 Change Management Policy	4
35.1 Executive Summary	4
35.2 Purpose	4
35.3 Scope	4
35.4 Change Management Policy Statements	5
35.4.1 Document the Change Request	5
35.4.2 Formal Assessment and Approval	6
35.4.3 Testing	6
35.4.4 Implementation	6
35.4.5 Review and Closure	7
35.5 Roles & Responsibilities	7
35.5.1 Change Requesters (Operations and/or IT)	7
35.5.2 Application Teams	7
35.6 Compliance	7
35.7 Exceptions	7
35.8 Review & Updates	7
35.9 References	7
35.9.1 RXO References	7
35.9.2 External References	8
35.10 Definitions	8

35 Change Management Policy

35.1 Executive Summary

Information Technology (IT) change management increases awareness and understanding of proposed IT changes, including any potential risks and business or security impacts. IT change management ensures that we make IT changes in a way that is better for IT systems, services, and the people who use them, reducing adverse impacts to our security posture or the quality of the services we provide.

35.2 Purpose

The purpose of this Policy is to:

- Describe what needs to happen before making a change to reduce the risk to other systems and services,
- Reduce incidents, service interruptions, and rework,
- Support notification to affected people in advance of any change, and
- Set requirements for RXO units making changes that tell them how to comply with IT Security obligations.

35.3 Scope

This policy applies to any person and business unit responsible for material changes to production IT systems, applications, and services for the company, including RXO, Inc., all subsidiaries, divisions, and operating entities. All directors, officers, full-time and part-time employees, agents, contractors, and third parties acting on behalf of RXO must comply with this policy.

Examples of changes covered by this policy include:

- Changes to service assets and Configuration Items (CIs) across the entire service lifecycle in the production or Disaster Recovery (DR) environments.
- Activities that impact an in-production application or system.
- Activities that require production applications/systems to be taken offline (even in a redundant configuration).
- Activities that could lead to an interruption of service if it fails.
- OS and Database upgrades or patches in any environment (prod and non-prod).
- Any modifications or service-impacting maintenance to network and storage environments since they share both Production and non-Production traffic, except an administrative property change which would not impact users and are more data entry modification based (e.g., they don't change how the system operates).
- Scheduled reboots of servers or restarts of services must have Change Records to establish, modify, or remove the scheduled restart/reboot.

- Changes to a Cost Center, Contract Service Level (metal classification) or System Status, which are considered controlled attributes, when projects are moving systems into an ongoing operational support mode or when systems are being decommissioned.
- Changes that include the addition, modification, or removal of authorized, planned, or supported service or CI and its associated documentation.
- Project related Changes that occur to service components as a result of Release to Production (RTP) implementations.
- Changes related to Security-related events (including service access attack or virus detection updates).
- Changes to RXO IT Service Management processes shall be approved and implemented via the processes outlined in this Change Management PPM.

Examples of changes that are out of scope of this policy include:

- Access Management activities (providing access to, adjusting access for, and removing access from) for services, systems, or configuration items.
- Changes that only affect one person (such as a password reset, directory permissions, or DL change) where no service impact will occur.
- Changes to production administrative servers where no SLA or element of RXO Logistics service depends on it being available (e.g., IBM's Managed Print Service report server).
- Reboots and service restarts used to restore service without implementing configuration changes (these are covered by the incident record(s) documenting the issue).
- Contract or Service Operations Changes will follow formal change control but within the Contract Management Process, Business Relationship Management Process, or overall Service Strategy discussions at the IT Governance level. This is due to monetary, confidentiality, or modification of business opportunities issues.
- Organizational Changes, which are managed outside of this process.

35.4 Change Management Policy Statements

35.4.1 Document the Change Request

- 35.4.1.1 Change requests must be documented in our ticketing system, currently Service-Now and/or JIRA.
- 35.4.1.2 Describe the purpose and intended outcome of the change.
- 35.4.1.3 Document who requested the change.
- 35.4.1.4 Document the systems, user groups, and business units impacted by the change.
- 35.4.1.5 Categorize the change, with at last normal and emergency as categories.

- 35.4.1.6 Describe the size, level of difficulty, or complexity of the change.
- 35.4.1.7 Describe the risks and benefits associated with making the change and with not making the change, including why the benefits outweigh the risks.
- 35.4.1.8 Quantify the risks as to probability and potential impact.
- 35.4.1.9 Assess and document whether there are any impacts to system security.
- 35.4.1.10 Document the technical changes being made (a technical design document).
- 35.4.1.11 Document the owners, resources, and approvers required to make the change.
- 35.4.1.12 Document a schedule to complete the changes.
- 35.4.1.13 Document a rollback plan for undoing the change if required.
- 35.4.1.14 Document the rollback triggers – the ways to tell that the changes are not successful and must be rolled back.
- 35.4.1.15 Update any user documentation to reflect the changes.

35.4.2 Formal Assessment and Approval

- 35.4.2.1 Non-emergency changes must be presented to and approved by the Change Advisory Board (CAB).

35.4.3 Testing

- 35.4.3.1 A documented test plan should be created listing all test scenarios and expected results.
- 35.4.3.2 Testing should be tracked showing the results for each test.
- 35.4.3.3 A final test report should be created showing the results of the tests.
- 35.4.3.4 Testing must be completed in a test environment, not in production.
- 35.4.3.5 Production data must not be used for testing without management approval, and it must be securely deleted from the test environment at the completion of testing if approved.

35.4.4 Implementation

- 35.4.4.1 Designated approvers must update the ticketing system of record to show approval of any change prior to the change being implemented in production environments.
- 35.4.4.2 Approvers are expected to review the design documentation and test results.
- 35.4.4.3 Approvers are expected to ensure a documented rollback plan exists.
- 35.4.4.4 Approvers should make certain that user documentation has been updated if the changes impact the end users.
- 35.4.4.5 Any impacts to security controls must be documented, reviewed, and approved.

35.4.5 Review and Closure

- 35.4.5.1 Once the change has been completed successfully in production, and it has been determined that rollback will not be necessary, the ticket should be closed in the ticketing system of record.

35.5 Roles & Responsibilities

35.5.1 Change Requesters (Operations and/or IT)

- 35.5.1.1 Ensure all change requests are documented as required in this Standard.

35.5.2 Application Teams

- 35.5.2.1 Ensure all changes are documented, tested, and approved as required in this Standard.

35.6 Compliance

Non-compliance with this policy may result in access restrictions to affected systems or disciplinary actions as per RXO's guidelines.

35.7 Exceptions

Any exceptions to this policy must be approved in writing by the RXO Governance Risk and Compliance (GRC) team and must include a valid business justification.

35.8 Review & Updates

This policy will be reviewed annually, or upon major infrastructure or threat landscape changes, or as required due to changes in business or technical requirements.

35.9 References

35.9.1 RXO References

- 35.9.1.1 RXO Operations Security Policy

35.9.2 External References

- 35.9.2.1 NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations
- 35.9.2.2 ISO/TS 10020 Quality Management Systems – Organization Change Management – Processes
- 35.9.2.3 ITIL 4 Change Management Process Guide
- 35.9.2.4 Project Management Institute’s Project Management Book of Knowledge – Change Management Process

35.10 Definitions

Change	The addition, modification, or deletion of any configuration or code that could impact the security, operation, or performance of RXO IT systems or services.
CAB	Change Advisory Board
NIST SP	National Institute of Standards and Technology Special Publication
ISO	International Standards Organization
TS	Technical Specification
ITIL	Information Technology Infrastructure Library

Certificate of Review

Change Management Policy

July 2nd 2026 2:10:56 pm

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Wednesday, April 15, 2026 11:06 AM EDT
Faisal Khan		Policy Approver	Approved	Tuesday, June 30, 2026 12:26 PM EDT
Mark Gutman		Policy Admin	Published	Thursday, July 2, 2026 2:10 PM EDT