



Disaster Recovery and Business Continuity Policy

DOC-IT-IS-17
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	Addition of 17.2.1.1.C
2.1	11/01/2025	RXO, Inc. updates, annual review

Table of Contents

17.0 Disaster Recovery and Business Continuity Policy	4
17.0.1 Purpose.....	4
17.0.2 Scope	4
17.0.3 BC/DR Roles and Responsibilities	4
17.1 Information Security and Business Continuity	5
17.1.1 Planning Information Security Continuity.....	5
17.1.2 Implementing Information Security Continuity	5
17.1.3 Verify, Review and Evaluate Information Security Continuity.....	6
17.2 Disaster Recovery - Redundancies	6
17.2.1 Availability of Information Processing Facilities	6

17.0 Disaster Recovery and Business Continuity Policy

17.0.1 Purpose

17.0.1.1 The purpose of the RXO, Inc. (RXO) Disaster Recovery and Business Continuity Policy (BC/DR) is to define the requirements regarding recovering from significant operational interruptions in a timely manner while minimizing business impacts.

17.0.2 Scope

17.0.2.1 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.

17.0.2.2 This policy encompasses all phases of the disaster recovery and business continuity lifecycle, from initial identification of critical systems to the regular testing of response plans and provides the appropriate information security requirements needed to perform these lifecycle activities.

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

17.0.3 BC/DR Roles and Responsibilities

Group Responsible for Establishing Controls	Control
Global Security Office	- Establish Disaster Recovery and Business Continuity Security Policy and standards. - Establish information security and business continuity standards, including planning, implementing, verifying, and reviewing and evaluating information security, business continuity controls. - Establish disaster recovery standards, including system redundancies, and availability of information processing facilities. Evaluate, review, and approve all requests for exceptions and variances of Disaster Recovery and Business Continuity Security Policy, standards, and procedures. - Annually review and update this policy.
It Operations Group	- Develop and maintain Disaster Recovery and Business Continuity procedures. - Manage Disaster Recovery and Business Continuity Security processes and resources. - Enforce adherence to information security and business continuity standards, including planning, implementing, verifying, and reviewing and evaluating information security, business continuity controls.

Group Responsible for Establishing Controls	Control
	- Enforce adherence to disaster recovery standard, including system redundancies, and availability of information processing facilities. - Facilitate and participate in the evaluation of requests for exceptions and variances of Disaster Recovery and Business Continuity Security Policy, standards, and procedures

17.1 Information Security and Business Continuity

17.1.1 Planning Information Security Continuity

17.1.1.1 RXO must determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

17.1.1.1.A RXO management is responsible for determining whether the continuity of information security is captured within the business continuity management process or within the disaster recovery management process.

17.1.1.1.B Information security requirements must be determined when planning for business continuity and disaster recovery plans.

17.1.1.1.C Information Security requirements remain the same in adverse situations unless otherwise documented. In addition, business impact analysis reviews must be performed for information security aspects to determine the information security requirements applicable to adverse situations.

17.1.1.1.D RXO must develop and implement business continuity plans (BCPs) for each of the company's business functions. (Adapted from RXO DOC 25116 Business Continuity Policy – 2.1 Policy Statement)

17.1.2 Implementing Information Security Continuity

17.1.2.1 RXO must implement, and maintain processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation. During disaster recovery events, users shall only be provided with access to the network and network services that they have been specifically authorized to use.

17.1.2.2 RXO must conduct periodic disaster recovery exercises to determine their readiness with personnel, process, computer systems, and security controls to identify any potential weaknesses that may affect our ability to recover from a business interruption. Business functions must test their respective BCPs on an annual basis. (Adapted from RXO DOC 25116 Business Continuity Policy – 2.1 Policy Statement)

17.1.3 Verify, Review and Evaluate Information Security Continuity

17.1.3.1 RXO must verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

17.1.3.1.A Organizational, technical, procedural, and process changes, whether in an operational or continuity context, can lead to changes in information security continuity requirements. The continuity of processes, procedures, and controls for information security must be periodically reviewed against these changed requirements.

17.1.3.1.B The RXO Business Continuity Management Program (BCMP) must be an organization-wide initiative and all employees, suppliers and service providers must be expected to contribute to this ongoing effort: (Adapted from RXO DOC 25116 Business Continuity Policy – 2.1 Policy Statement)

17.2 Disaster Recovery - Redundancies

17.2.1 Availability of Information Processing Facilities

17.2.1.1 Information processing facilities must be implemented with redundancy sufficient to meet availability requirements.

17.2.1.1.A All business requirements for the availability of information systems must be identified. Where the availability cannot be guaranteed using the existing systems architecture, redundant components, or architectures must be considered.

17.2.1.1.B Where applicable, redundant information systems must be tested to ensure the failover from one component to another component performs as intended.

17.2.1.1.C RXO must ensure that all third-party vendors and service providers who support critical business functions have robust disaster recovery and business continuity plans. These plans must be reviewed periodically, and service level agreements (SLAs) should include provisions for recovery times in the event of an interruption.

Certificate of Review

Disaster Recovery and Business Continuity Policy

December 18th 2025 10:29:38 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 3:32 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:00 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:29 AM EST