



Security Incident Response Policy

DOC-IT-IS-16
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

16.0 Security Incident Response Policy.....	4
16.0.1 Purpose.....	4
16.0.2 Scope	4
16.1 Management of Information Security Incidents and Improvements.....	4
16.1.1 Responsibilities and Procedures.....	4
16.1.2 Reporting Information Security Events.....	5
16.1.3 Reporting Information Security Weaknesses	5
16.1.4 Assessment of and Decision on Information Security Events.....	5
16.1.5 Response to Information Security Incidents.....	6
16.1.6 Learning from Information Security Incidents.....	6
16.1.7 Collection of Evidence	6

16.0 Security Incident Response Policy

16.0.1 Purpose

16.0.1.1 The purpose of the RXO, Inc. (RXO) Security Incident Response Policy is to define information security requirements to minimize the impact of unplanned events that may affect quality, reliability, availability, and overall security of organizational data, applications, and systems. The contents of this policy provide for a controlled, repeatable, efficient, and comprehensive handling approach for all incidents and outages. This document should be reviewed in conjunction with the **Cyber Security Incident Response Plan** which details the RXO incident response process.

16.0.2 Scope

16.0.2.1 This policy applies to all RXO subsidiaries, divisions, and operating entities, employees, agents, contractors, and third-party partners, as well as all data and systems used by or supporting the company.

16.0.2.2 This policy encompasses all phases of incident response management.

16.0.2.3 The policy applies to all sensitive information and other classes of protected information.

16.1 Management of Information Security Incidents and Improvements

16.1.1 Responsibilities and Procedures

16.1.1.1 Management responsibilities and procedures must be established to ensure a quick, effective, and orderly response to information security incidents.

16.1.1.1.A A formalized security incident response program must be in place to ensure that those responsible for information security incident response are clearly identified and understand RXO's priorities for handling information security incidents.

16.1.1.1.B Responsibilities defined within the RXO security incident response program must address the entire incident response lifecycle, including, but not limited to preparation; identification; notification; containment; analysis; eradication; recovery; and lessons learned. The communication phase includes the escalation, controlled recovery from an incident and informing internal and external parties. All communication must be approved and permitted by the legal department prior to any notification to external parties.

16.1.1.1.C Formally defined and staffed team(s) must provide investigative and response support to identified security events that are suspected of being incidents. All responsible members of the incident response team(s) must be sufficiently trained and tested to ensure that they possess sufficient competency to support the required activities.

16.1.1.1.D All incidents, from initial investigation throughout the response lifecycle, must be properly documented. This reporting must include the completion of applicable information security event reporting documentation used to capture the details of the investigation,

containment, root cause analysis, and mitigation activities. These reports must be completed and reviewed by the incident response team for content at the end of any incident investigation to provide an environment dedicated to constant awareness and programmatic update.

16.1.1.1.E This policy will be reviewed and updated annually or as required by changes in regulatory or business requirements.

16.1.2 Reporting Information Security Events

16.1.2.1 Information security events must be reported through appropriate management channels as quickly as possible.

16.1.2.1.A All users must be made aware of their responsibility to report potential information security events as quickly as possible. They must also be made aware of the procedures for reporting information security events and how to contact and interact with the appointed escalation chain responsible for incident investigation.

16.1.2.1.B As part of the incident response reporting process, users should consider several topical areas that could constitute a potential security issue. These include: the suspected presence of ineffective security controls; potential breaches of information integrity, confidentiality, or availability; human errors; noncompliance with policies or guidelines; breaches of physical security arrangements; uncontrolled or unapproved system changes; malfunctions of software or hardware; and access violations.

16.1.3 Reporting Information Security Weaknesses

16.1.3.1 Employees and contractors using RXO's information systems and services must note and report any observed or suspected information security weaknesses in systems or services.

16.1.4 Assessment of and Decision on Information Security Events

16.1.4.1 Information security events must be assessed, and it must be decided if they are to be classified as information security incidents.

16.1.4.1.A Upon notification, members of the RXO Corporate Security Operations Center (CSOC) and Digital Forensics and Incident Response Team (DFIR) will assess each information security event using the Incident Severity Classification identified in the Cyber Security Incident Response Plan. Upon completion of this review, the CSOC/DFIR representatives must determine if the event qualifies as a formal information security incident and direct it for closure or further actions.

16.1.4.1.B The results of the security event criticality assessment and decision must provide complete details for the purpose of future reference and verification analysis. This information will be included in any final reporting generated by the DFIR team at the conclusion of the investigation should the criticality of the event warrant a formal report.

16.1.5 Response to Information Security Incidents

16.1.5.1 Information security incidents must be responded to in accordance with the documented procedures.

16.1.5.1.A Once an incident has been formally declared, the RXO CSOC/DFIR as well as any adjunct support personnel must operate in accordance with the defined incident response workflows and direction from the incident commander as defined in the RXO Cyber Security Incident Response Plan.

16.1.5.1.B Incident activities must include: the collecting of evidence as soon as possible after the occurrence; conducting information security forensics analysis (when appropriate); escalation, as required; ensuring that all involved response activities are properly logged for later analysis; communicating the existence of the information security incident or any relevant details thereof to other internal and external individuals or organizations with a need-to-know; dealing with information security weakness(es) found to cause or contribute to the incident; and, once the incident is successfully dealt with, formally closing and recording it.

16.1.6 Learning from Information Security Incidents

16.1.6.1 Knowledge gained from analyzing and resolving information security incidents must be used to reduce the likelihood or impact of future incidents.

16.1.7 Collection of Evidence

16.1.7.1 RXO must define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

16.1.7.1.A Procedures for evidence collection must provide processes for the identification, collection, acquisition, and preservation of evidence in accordance with different types of media, devices, and status of devices, e.g., powered on or off. The procedures must address the chain of custody, safety of evidence, safety of personnel, roles, and responsibilities of personnel involved, competency of personnel, documentation creation and retention and status briefing for collecting evidence.

16.1.7.1.B Personnel involved in digital evidence handling must be properly trained and evidenced by the possession of relevant certification in computer forensics, or other relevant means of qualification, and is required for personnel as well as the operation of tools used during the acquisition of evidence, to strengthen and preserve the evidence chain of custody.

16.1.7.1.C Forensic evidence may transcend RXO or jurisdictional boundaries. In such cases, all necessary forensic evidence and associated information must be collected in a manner that is supported by RXO legal rights. The company's evidence collection practices must also encompass those activities necessary to maximize the opportunities for successful legal actions across the relevant jurisdictions.

Certificate of Review

Security Incident Response Policy

December 18th 2025 10:28:51 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 4:33 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 10:59 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:28 AM EST