



Operations Security Policy

DOC-IT-IS-12
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 Review
2.1	11/01/2025	RXO, Inc updates, annual review

Table of Contents

12.0 Operations Security Policy	4
12.0.1 Purpose	4
12.0.2 Scope	4
12.1 Operational Procedures and Responsibilities	4
12.1.1 Documented Operating Procedures	4
12.1.2 Change Management	4
12.1.3 Capacity Management	5
12.1.4 Separation of Development, Testing and Operational Environments	5
12.2 Protection from Malware	5
12.2.1 Controls against Malware	5
12.3 Backup	5
12.3.1 Information Backup	5
12.4 Logging and Monitoring	6
12.4.1 Event Logging	6
12.4.2 Protection of Log Information	6
12.4.3 Administrator and Operator Logs	6
12.4.4 Clock Synchronization	7
12.5 Control of Operational Software	7
12.5.1 Installation of Software on Operational Systems	7
12.6 Technical Vulnerability Management	8
12.6.1 Management of Technical Vulnerabilities	8
12.6.2 Restrictions on Software Installation	8
12.7 Information Systems and Audit Considerations	8
12.7.1 Information Systems Audit Controls	8

12.0 Operations Security Policy

12.0.1 Purpose

12.0.1.1 The purpose of the RXO, Inc. (RXO) Operations Security Policy is to provide information security requirements for the processes related to operating within RXO systems and applications.

12.0.2 Scope

12.0.2.1 This policy applies to all RXO subsidiaries, divisions, and operating entities, all employees, agents, contractors, and third-party partners.

12.0.2.2 This policy encompasses operational procedures and responsibilities, protection from malware, backups, logging, and monitoring, control of operational software, technical vulnerability management and information systems and audit consideration.

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

12.1 Operational Procedures and Responsibilities

12.1.1 Documented Operating Procedures

12.1.1.1 Operating procedures must be documented and made available to all personnel who need them.

12.1.1.1.A Documented procedures must be developed, documented and implemented for operational activities associated with information processing and communication facilities, such as computer start-up and shut-down procedures, backup, equipment maintenance, media handling, computer room management and safety.

12.1.1.1.B Operating procedures and the procedural documentation for system activities must be formally maintained, with changes to the documents subjected to version control with formal authorization by management. Where technically feasible, these procedures must mandate that information systems be managed in a consistent manner, using the same procedures, tools, and utilities.

12.1.2 Change Management

12.1.2.1 Changes to the organization, business processes, information processing facilities, and systems that affect information security must be controlled to ensure that all modifications to information processing facilities and systems are managed and recorded through formal change management processes. All major changes must include a security impact analysis to identify potential risks.

12.1.3 Capacity Management

12.1.3.1 The use of resources must be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

12.1.3.1.A System and resource capacity concerns must be monitored and addressed in order to provide a sustainable infrastructure.

12.1.3.1.B All systems must be continuously reviewed to ensure that their capabilities remain in alignment with the expected capacity requirements. These reviews must include considerations for system tuning and monitoring needed to improve the availability and efficiency of systems. Detective controls must be implemented to provide alerts for new or emerging system performance issues. Projections of future capacity requirements must take into account current activities, new business and system requirements, and projected trends affecting the information processing capabilities.

12.1.3.1.C Specific monitoring must be implemented with regard to the utilization of any system resources with lengthy procurement lead times or high costs to allow for earlier identification of potential issues as well as usage trends.

12.1.3.1.D Reviews of information must be used to identify and avoid potential bottlenecks, dependence on key personnel that might present a threat to system security or services and address planning for RXO mission critical system implementations.

12.1.4 Separation of Development, Testing and Operational Environments

12.1.4.1 Development, testing, and operational environments must be separated to reduce the risks of unauthorized access or changes to the operational environment to allow for sufficient and appropriate privileges while maintaining appropriate security and resilience controls.

12.2 Protection from Malware

12.2.1 Controls against Malware

12.2.1.1 Detection, prevention, and recovery controls to protect against malware must be implemented based on a combination of detective and preventative tools, information security awareness, and appropriate system access and change management controls. Malware protection tools must be continuously updated, and endpoints must be protected using Endpoint Detection and Response (EDR) solutions.

12.3 Backup

12.3.1 Information Backup

12.3.1.1 Backup copies of information, software, and system images must be taken and tested regularly in accordance with an agreed backup standard.

12.3.1.1.A The retention and protection requirements for the backup of information, software, and systems must be defined and maintained. Backups must be encrypted both in transit and at rest.

12.3.1.1.B Operational procedures must mandate the monitoring of the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup standard.

12.3.1.1.C Backup arrangements for individual systems and services must be regularly tested to ensure that they meet the requirements of business continuity plans. In the case of critical systems and services, backup arrangements must cover all systems information, applications, and data necessary to recover the complete system in the event of a disaster.

12.4 Logging and Monitoring

12.4.1 Event Logging

12.4.1.1 Event logs recording user activities, exceptions, faults, and information security events must be produced, kept, and regularly reviewed.

12.4.1.1.A Event logs must be maintained for all systems and applications, as determined through risk assessment practices that consider functionality, business criticality, and sensitivity of the information stored, processed, and/or transmitted through the system. At the minimum this applies to system components including but not limited to: All DMZ systems, domain controllers, end routers and firewalls, all security technologies, DNS, Mail infrastructure, and storage systems. Event logs must be centralized into a Security Information and Event Management (SIEM) system for timely detection and analysis of security incidents.

12.4.1.1.B Event logs must contain sufficient detail to provide evidence of activities and user identity. Such details must be defined through assessed value or compliance objectives. Logs must comply with data retention and privacy policies, ensuring personally identifiable information (PII) is handled appropriately.

12.4.2 Protection of Log Information

12.4.2.1 Logging facilities and log information must be protected against tampering and unauthorized access.

12.4.2.1.A Controls must be implemented to protect against unauthorized changes to log information and operational problems with the logging facility.

12.4.2.1.B Audit logs must be archived due to record retention or other requirements to collect and retain log evidence.

12.4.3 Administrator and Operator Logs

12.4.3.1 System administrator, privileged user accounts and system operator activities must be logged and the logs protected and regularly reviewed and controls must be implemented so that logs are protected and reviewed to ensure their integrity and maintain the accountability for all activities. Privileged accounts must use Multi-Factor Authentication (MFA).

12.4.4 Clock Synchronization

12.4.4.1 The clocks of all relevant information processing systems within an organization or security domain must be synchronized to a single reference time source that obtains its values from a reputable external source. Redundant solutions are acceptable so long as these devices are able to be relied on for exact replication of time values. Using time-synchronization technology, such as Network Time Protocol (NTP), all critical system clocks and times must be synchronized.

12.4.4.2 The processes governing external and internal requirements for time representation, synchronization, and accuracy must be developed, documented, and implemented. Such processes must include legal, regulatory, contractual and/or compliance requirements.

12.5 Control of Operational Software

12.5.1 Installation of Software on Operational Systems

12.5.1.1 Procedures must be implemented to control the installation of software on operational systems.

12.5.1.1.A Processes must be developed, documented, and implemented to control the implementation of and changes to software on operational systems. These processes must take into consideration appropriate job role responsibilities as well as change management requirements.

12.5.1.1.B All implemented software solutions must be regularly reviewed to maintain awareness of current and future vendor support options. In situations where the vendor(s) is planning to stop or has stopped regular support and maintenance, application and business owners must consider the risks and act accordingly. Vulnerability management and patch implementation is a requirement for RXO systems. If outdated or unsupported software results in un-patchable systems, then the software is required to be upgraded.

12.5.1.1.C Any decision to upgrade to a new release must take into account the business requirements for the change and the security of the release (e.g., the introduction of new information security functionality or the number and severity of information security problems affecting this version). Appropriate vulnerability management practices must be applied to ensure that software updates are regularly applied to remove or reduce information security weaknesses.

12.5.1.1.D Suppliers in support roles must only have physical or logical access according to their agreed-upon maintenance responsibilities. In general, this access must be restricted to times of absolute necessity and as approved by management. Audit and logging capabilities must be configured to provide sufficient detail of all external access into the RXO environment(s) and system(s) during support activities.

12.6 Technical Vulnerability Management

12.6.1 Management of Technical Vulnerabilities

12.6.1.1 Information about technical vulnerabilities of information systems being used must be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

12.6.1.1.A A current and complete inventory of assets must be maintained to support an effective technical vulnerability management strategy. Specific information must include the product vendor, version numbers, current state of deployment (e.g., what software is installed on what systems) and the person(s) responsible for the product. All RXO-managed Information Systems are in scope for periodic Vulnerability Scans, regardless of network segment, security zone, or physical location. Technical Owners must enroll all their systems with the vulnerability scanning tool.

12.6.1.1.B An effective management process for technical vulnerabilities must be developed, documented, and implemented.

12.6.1.1.C Roles and responsibilities associated with technical vulnerability management, must be established including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required.

12.6.2 Restrictions on Software Installation

12.6.2.1 Rules governing the installation of software by users must be established and implemented. Processes must be in place to define acceptable software installations. In all cases, there must be a Business justification for any software installation. For end-user computing, unless there is an approved exception, end-users are prohibited from having administrative rights to their system. Any requested application installation must be evaluated for the possibility of malware or malicious code.

12.7 Information Systems and Audit Considerations

12.7.1 Information Systems Audit Controls

12.7.1.1 Audit requirements and activities involving verification of operational systems must be carefully planned and agreed to minimize disruptions to business processes.

12.7.1.1.A Comprehensive plans must be developed, documented, and implemented to minimize the impact of audit activities on business processes and operational systems. The scope of technical audit tests and all requirements for access to systems and data must be clearly defined and agreed with all levels of applicable management.

12.7.1.1.B A limitation of read-only access to software and data must be enforced to protect production during audit testing. Requests for other than read-only access must only be allowed for isolated copies of system files.

12.7.1.1.C When an audit is complete, any isolated copies of system files must receive proper disposal in accordance with their data sensitivity and classification or given appropriate protection if there is an obligation to retain such files under audit documentation requirements.

12.7.1.1.D Audit tests that could affect system availability must occur outside business hours. Requirements for special or additional processing must be identified and approved. All access must be monitored and logged to produce an audit trail.

Certificate of Review

Operations Security Policy

December 18th 2025 10:20:54 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Monday, November 24, 2025 10:43 AM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 10:58 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:20 AM EST