



Vulnerability Management Standard

DOC-IT-IS-12-6
Revision 2.0
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	11/01/2025	Severity Scoring verbiage, remediation deadlines and frequencies, remediation coordination.

1	Introduction	4
1.1	Purpose	4
1.2	Scope	4
2	Standards.....	4
2.1	Policies for Information Security	4
2.2	Penetration Testing	5
2.3	Infrastructure Vulnerability Severity Scoring.....	5
2.4	Vulnerability Remediation Deadlines*	7
2.5	Frequencies.....	7
3	Roles and Responsibilities.....	7
3.1	Remediation Coordination.....	8
4.	Definitions	8

1 Introduction

1.1 Purpose

The purpose of the RXO, Inc. (RXO) Vulnerability Management Standard is to provide information security requirements for the processes related to management of security vulnerabilities within RXO systems and applications.

1.2 Scope

This Standard applies to:

- All of RXO, Inc., including all subsidiaries, divisions, and operating entities. All directors, officers, employees, contractors, and third parties acting on behalf of RXO must comply with this policy.
- All members of Information Technology, the Information Owners who represent the business's interests, and the people who support the daily operation of RXO Information Systems.
- All Information Systems, including network infrastructure, hardware, software, operating systems, and applications.

2 Standards

2.1 Policies for Information Security

- All RXO-managed Information Systems are in scope for periodic Vulnerability Scans and Vulnerability Assessments, regardless of network segment, security zone, or physical location. Technical Owners must enroll all their systems with the vulnerability scanning tool.
- Vulnerability Assessments may only be performed by a member of GSO or authorized delegates.
- Vulnerability assessment tools must be approved by the CISO.
- Access to vulnerability assessment tools must follow the access controls in DOC-IT-IS-09 Access Control Policy, specifically the principle of Least Privilege.
- Any new Information System that will access the RXO network must undergo a Vulnerability Scan before being allowed to "Go Live".
- All vulnerabilities classified as critical or high must be addressed before an Information System is connected to the RXO network.
- GSO may perform a Vulnerability Assessment after any Significant Change to an Information System.
- Vulnerability Assessments must be performed on all systems and applications as deemed necessary by GSO. See section 2.4 Vulnerability Assessment Frequency for frequency of assessments.

- Any information generated by a Vulnerability Assessment is classified as Sensitive and must be handled appropriately.
- GSO may, at their discretion, determine that a vulnerability must be handled as a security incident.
- Information Owners that are notified by GSO that vulnerabilities have been found on their Information System must remedy vulnerabilities in a timely manner, as defined in the Vulnerability Remediation Deadlines section below.
- Any Vulnerability that cannot meet the remediation period as defined in the standards is a Policy violation and will be subject to the Security Policy Exception process.
- All remediation activities must be properly documented, auditable, and adhere to the change management process.
- Remediation must be validated by a re-scan.

2.2 Penetration Testing

- GSO has the exclusive authority to perform penetration testing on any RXO network or system.
- Penetration Tests must be performed on all Internet-facing systems at least annually.
- Penetration Tests must have a written engagement plan that details the scope of the test, items that are expressly out-of-scope, the timeframe for the test, and the methods that may be used – for example, social engineering or a denial of service. The engagement plan must be approved by the CISO prior to any testing activity.
- All information included in the reports or artifacts created as part of the Penetration Test is classified as Sensitive and must be handled appropriately.
- Penetration Tests must be performed in a production environment unless an equivalent non-production environment is available.

2.3 Infrastructure Vulnerability Severity Scoring

- Infrastructure vulnerability severity scoring at RXO uses industry standard scoring methodology in combination with tool specific scoring systems.
- CVSS v3.x score: (<https://nvd.nist.gov/vuln-metrics/cvss>)
- CISA Known Exploited Vulnerability Catalog: (<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>) and Exploit Prediction Scoring System (https://www.first.org/epss/data_stats.html)

2.4 Vulnerability Remediation Deadlines*

Technical vulnerabilities are rated based on the risk they present to RXO. Required remediation timelines align with vulnerability ratings based on the table below.

		Timeline
Urgent	Presents clear and present danger to RXO and its associated systems. These are typically zero-day vulnerabilities with no mitigation and active exploitation in wild.	Must be remediated immediately (not to exceed 3 days)
Critical	Could allow code execution without user interaction resulting in unauthorized system or data access/loss. These have a high probability of exploitation and potential to impact confidentiality, availability, and integrity of our systems	Must be remediated within 15 days
High	Could result in compromise of one or more systems or data. Has few controls in place to mitigate and are easy to attack.	Must be remediated within 30 days
Medium	Could lead to an attacker obtaining system statistics, user accounts, or other sensitive information that would aid in an attack.	Must be remediated within 60 days
Low	Findings that have minimal impact to RXO. Maybe remediated based on system-maintained schedules.	May be remediated within 90 days

* NOTE: For patch releases, all timeframes start on the release date of patch and for other vulnerabilities found, timeframes start on the date of notification of vulnerability to the team responsible for remediation

2.5 Frequencies

- All servers and endpoints must apply security patching at least once a month.
- Application Vulnerability Assessment – Annually or with a Significant Change

3 Roles and Responsibilities

PROD APP TEAM - The Prod App Team is responsible for pushing and managing updates, communicating with App Owners, server decommission, and software changes in coordination with technical owners on maintenance windows.

GSO - The Information Security team is responsible for communication to all parties with accurate scan data, assisting with system changes when needed, and managing risk acceptance process.

SYSTEM EQUIPMENT STEWARD - The Technical Owner is responsible to confirm configuration changes, test proof and patch cycles, and the maintenance of their servers.

INFORMATION OWNER - The Information Owner is responsible for determining maintenance windows for their servers and for completion of the risk acceptance process when needed.

3.1 Remediation Coordination

To maintain the integrity of monthly security patching cycles and ensure consistent vulnerability remediation across environments, the following standard applies to all development and infrastructure activities:

- **Non-Interference with Patching Cycles**
Development work must not interfere with scheduled monthly security patching. All activities that affect server availability or configuration must be planned around the established patching schedule.
- **Coordination Requirement**
Any work impacting servers—including deployments, upgrades, migrations, or configuration changes—must be coordinated with the patching calendar maintained by the Global Command Center (GCC) or relevant patching team.
- **Exception Handling**
If a deviation from the patching schedule is required due to business-critical constraints, a formal security exception must be submitted and approved through the designated process (e.g., ServiceNow Security Exception module). Patching must resume the following weekend after the exception is granted and should not be deferred to the next month's scheduled cycle. Exception requests must be approved by a Director-level or higher leader within the requesting Business Unit prior to review by the Information Security team.

4. Definitions

Term	Definition
"Go Live"	The point where an Information System or solution starts to perform the process it was designed for. This is in contrast to the build phase where the initial configuration and installations take place.
Information System	A generalized term for all computers, laptops, mobile devices, network devices, hardware, software, operating systems, applications, tools, utilities, or vendor provided products.
Penetration Test	An intentional attack against a system to simulate how a malicious attacker would find and exploit vulnerabilities on the system. The test can be performed by either internal or external resources. Another commonly used term is "Red Team Exercise".

Risk Assessment	The process of identifying the risks to system security and determining the probability of occurrence, resulting impact, and additional controls that would mitigate this impact.
Security Policy Exception	An instance of non-compliance with RXO's Global Security Policies and a decision by senior management to accept the associated risks.
Significant Change	Significant changes are dependent upon the system or application. Examples include: • A change that alters the way that an Information System is accessed. • Changing the application architecture. • Platform or infrastructure changes, such as moving from an on-premise solution to a cloud solution. • Any change that has the potential to adversely affect the security of RXO information or the RXO network.
Technical Owner	The member of IT that is responsible for the day-to-day operation of an information system.
Vulnerability	A flaw or weakness in a system's design, implementation, management, or operation that could be exploited to gain unauthorized access to the system or information stored on that system.
Vulnerability Assessment	A review of the technical vulnerabilities present in an application or server. This may include a Vulnerability Scan, code review, or a review of the application's architecture and communication security.
Vulnerability Scan	An automated test of known vulnerabilities that can be found in an application or server. For the purpose of this policy, network and port scanning are included in this definition.

Certificate of Review

Vulnerability Management Standard

December 18th 2025 10:21:38 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 12:38 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 10:58 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:21 AM EST