



Secure Port Usage Standard

DOC-IT-IS-28
Revision 1.1
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	8/20/2025	Initial Version
1.1	11/1/2025	RXO, Inc Revisions

Table of Contents

1 Executive Summary	4
2 Purpose.....	4
3 Scope.....	5
4 Standard Statements	6
4.1 Approved Secure Ports	6
4.2 Port Management.....	7
4.3 Encryption Enforcement.....	7
4.4 Monitoring and Logging.....	7
4.5 Vulnerability Management.....	7
5 Review and Updates.....	7
6 References.....	7

4 Executive Summary

This document establishes the standard for secure port usage within RXO to mitigate risks associated with unauthorized access, data breaches, and service disruptions. Open network ports are common attack vectors exploited by malicious actors. By defining acceptable port configurations and usage policies, this standard aims to strengthen the RXO's cybersecurity posture and ensure compliance with industry best practices and regulatory requirements.

The standard applies to all systems, applications, and network devices managed by RXO, including on-premises infrastructure and cloud environments. It supports the broader goals of the Information Security Management System (ISMS) and aligns with frameworks such as ISO/IEC 27001, NIST SP 800-53, and CIS Controls.

5 Purpose

This standard defines standards for the secure configuration and management of network ports at RXO. Its goal is to ensure encrypted communication, minimize exposure to cyber threats, and maintain compliance with industry best practices.

- **Port scanning** must be conducted regularly to identify unauthorized open ports.
- **Firewall rules** must enforce least privilege access to approved ports.
- **Change control** procedures must be followed before opening any new port.
- **Logging and monitoring** must be enabled for all traffic on approved ports.
- Use **network segmentation** to isolate sensitive systems.
- Implement **intrusion detection/prevention systems (IDS/IPS)** to monitor port activity.
- Enforce **multi-factor authentication (MFA)** for services exposed via secure ports.

6 Scope

This standard applies to:

- All RXO entities, employees, contractors, consultants, temporary workers, and third-party partners managing or accessing RXO's IT infrastructure.
- All networked systems including servers, workstations, firewalls, routers, switches, and cloud-hosted services.
- All environments: production, development, testing, and staging.

Excluded

- Personal devices not connected to the corporate network.
- Temporary lab environments explicitly approved by the Information Security team.

7 Standard Statements

7.1 Approved Secure Ports

7.1.1 All The following ports are approved for use in RXO's environments:

Port	Usage	Protocol	Requirements
22	Remote Administration	SSH	Key-based authentication, MFA, root login disabled
53	Domain Resolution	DNS	Must use RXO-approved DNS servers; DNSSEC preferred
853	Encrypted DNS	DNS over TLS	TLS 1.2+ required; use RXO-approved resolvers
445	Server Message Block	SMB	SMBv3 only; Internal use only
67/68	Dynamic IP Addressing	DHCP	Only authorized DHCP servers/clients; monitor for rogue DHCP
80	Web-redirection only	HTTP	Must Redirect to HTTPS: no sensitive data
443	Web traffic	HTTPS	TLS 1.2 or higher; valid CA certs; HSTS preferred
2049	Network File System	NFS	Use Kerberos with NFS4
514	Logging	Syslog	Authorized Servers only; Internal use only
5986	Remote Management	WinRM	Restrict access to trusted networks; internal only
3389	Remote access	RDP	Internal Only; MFA required; whitelisted IPs only
1494,2598	Citrix ICA Traffic	Citrix	Use SecureICA where possible
465	Mail Transfer	SMTPS	TLS required; must use RXO-approved mail relay
636	Directory services	LDAPS	TLS required; plaintext LDAP (389) not permitted
989/990	File transfers	FTPS	TLS required; plain FTP (21/20) prohibited
993	Email retrieval	IMAPS	TLS Enforced
995	Email retrieval	POP3S	TLS Enforced
123	Time synchronization	NTP/NTS	Only to authorized NTP servers; authenticated where possible
161/162	Network Mon	SNMPv3	SNMP v1 and v2 are prohibited
587	Email submission	SMTP Submission	STARTTLS required
3306	DB Access	MySQL	Only between app and DB servers; TLS required
1433	DB Access	MS SQL	Only between app and DB servers; TLS required
5432	DB Access	PostgreSQL	Only between app and DB servers; TLS required
18091/18092	CouchBase	Couchbase	Only with encryption enabled.
50051	API communication	gRPC	Must use TLS (mTLS preferred); restrict to internal services

Any use of ports outside this list must be approved by Business Information Security Officer (BISO) and documented with justification.

7.2 Port Management

- 7.2.1 The Disable unused ports on all systems and devices.
- 7.2.2 Restrict access using firewalls, access control lists (ACLs), and network segmentation.
- 7.2.3 Implement port security on switches to prevent unauthorized device connections.

7.3 Encryption Enforcement

- 7.3.1 All services exposed via open ports must use secure protocols (e.g., TLS 1.2 or higher). Unencrypted protocols (e.g., Telnet, FTP, HTTP) are prohibited.

7.4 Monitoring and Logging

- 7.4.1 All port activity must be logged and monitored via a Security Information and Event Management (SIEM) system.
- 7.4.2 Alerts must be generated for unauthorized scans, traffic anomalies, or configuration changes.

7.5 Vulnerability Management

- 7.5.1 Conduct regular scans to identify open ports and assess risks.
- 7.5.2 Remediate findings within 30 days or submit a risk acceptance form to the BISO.

8 Review and Updates

This standard will be reviewed annually or upon major infrastructure or threat landscape changes.

9 References

- NIST SP 800-215: Guide to Enterprise Network Security
- NSA Network Infrastructure Security Guide

Certificate of Review

Secure Port Usage Standard

December 18th 2025 10:43:38 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 10:56 AM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:25 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:43 AM EST