



Remote Access Management Standard

DOC-IT-IS-06-2-1
Revision 2.0
NOVEMBER 1, 2025

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	RXO, Inc. Revisions, annual review

1 Executive Summary	4
2 Purpose.....	4
3 Scope.....	4
4 Remote Access Management Standard	5
4.1 General Standards	5
4.2 Technical Standards.....	5
5 Definitions	6

1 Executive Summary

Providing Remote Access exemplifies the tradeoff between security and convenience. Allowing Remote Access to the RXO network means that the user does not have to be physically present at an RXO location. However, Remote Access opens a potential avenue for attackers to gain unauthorized access to RXO resources. Striking this balance allows RXO to remain secure while embracing the benefits of remote information systems.

2 Purpose

The purpose of the RXO Remote Access Standard is to provide information security requirements for the processes related to remotely connecting to the RXO network and resources.

3 Scope

This standard applies to RXO, Inc., including all subsidiaries, divisions, and operating entities. All people who connect to RXO Information Systems through Remote Access, including but not limited to all directors, officers, employees, agents, contractors, and third parties acting on behalf of RXO must comply with this policy.

All Information Systems, including network infrastructure, hardware, software, operating systems, and applications that use or support Remote Access capabilities. Applications or resources that are accessible from the public internet are out of scope.

4 Remote Access Management Standard

4.1 General Standards

- Remote Access is subject to all RXO policies, including the Acceptable Use Policies (DOC-IT-IS-19 and DOC-IT-IS-20), the Access Controls Policy (DOC-IT-IS-09).
- All Remote Access connections require Multi-Factor Authentication.
- Multi-Factor Authentication solutions must be approved by Information Security.
- Remote Access configuration information must not be shared publicly.
- Only RXO managed devices may connect to the internal RXO network via full tunnel VPN.
- Non RXO managed devices may only connect to specific applications and folders.
- Only systems with approved operating systems and anti-malware software may be used to remotely connect to the RXO network. Operating systems and anti-malware signatures must be up to date.
- Devices connecting to the RXO network must be patched to current levels.
- Connections from non RXO managed devices must be logged and auditable.
- RXO may limit or block Remote Access to high-risk systems or resources.
- Employee Remote Access privileges must be approved by the requestor's manager.
- Third party Remote Access Privileges must be approved by the relevant Business Information Security Officer (BISO).
- Non-employees (contractors, consultants, partners, and suppliers) must be covered under a Non-Disclosure Agreement (NDA) before connecting to the RXO network.

4.2 Technical Standards

- Remote Access connections must terminate in a DMZ.
- Anonymous Remote Access connections are not allowed.
- Password caching must be disabled on all Remote Access clients.
- Privileged Accounts may not connect to the RXO network through Remote Access methods.
- All Remote Access technologies must be approved by the relevant BISO.
- All Remote Access connections to the RXO network must be configured to prevent Split Tunneling.
- Remote Access sessions must be encrypted.
- All Client VPN Remote Access sessions must have a maximum session duration of no more than 24 hours.

5 Definitions

Term	Definition
Information System	A generalized term including but not limited to computers, laptops, mobile devices, network devices, hardware, software, operating systems, applications, stored information, tools, utilities, or vendor provided products.
Multi-Factor Authentication	The process of proving identity by providing at least two identifying items. These factors include: • 'Something you Know', e.g., a password • 'Something you Are', e.g., a biometric identifier such as a fingerprint • 'Something you Have', e.g., an access token (hardware or software) Using multiple types of a single factor, a password and security question, does not qualify as multi-Factor.
Privileged Accounts	An account that is granted special access to an Information System. This includes administrator accounts, root accounts, or super user accounts.
Remote Access	The process of connecting to the RXO network through any network connection that is not managed by RXO.
Split-Tunneling	Simultaneous direct access to a non-RXO network (such as the Internet, or a home network) from a device while remotely connected to RXO's corporate network.
Virtual Private Network (VPN)	A secure method for accessing a remote, private network that uses the Internet or other untrusted, public network to transmit data. A VPN uses authentication and encryption to maintain privacy and security.
Client VPN	A VPN connection made from a remote computer, laptop, or other device. These connections are made to allow individual users to connect to network resources as if they were on-site.
Site-to-Site VPN	A VPN connection created to extend the RXO network to a remote site. These connections allow users to connect to the remote site's Local Area Network (LAN) and access resources without initiating a Client VPN connection.

Certificate of Review

Remote Access Management Standard

December 18th 2025 10:12:12 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Monday, November 24, 2025 1:36 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 10:57 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:12 AM EST