



Network Segmentation Standard

DOC-IT-IS-13-1-3

Revision 2.1

APRIL 14, 2026

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 © 2026 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	RXO, Inc. Revisions, annual review, additional zones & controls
2.1	04/14/2026	Added geographical zones

Table of Contents

1 Executive Summary4

2 Purpose.....4

3 Scope.....4

4 Network Segmentation Standard5

 Network Zones5

 Security Levels6

 Inter-zone Communication and Access Controls7

 Site-to-Site Communications.....8

 External Access to Systems8

 Internal Network Safeguards9

1 Executive Summary

Network Segmentation is the concept of limiting communications and service / functions to only the protocols and device access necessary to facilitate business capabilities and management. Network segmentation is a highly effective control that limits the impact of a network intrusion and makes it significantly more difficult for an adversary to locate and gain access to RXO's most sensitive information. It also increases the likelihood of detecting an adversary's activity in a timely manner.

2 Purpose

The purpose of the RXO Network Segmentation Standard is to provide information security requirements for the segregation of information and systems using network segmentation. This standard defines the network zones used for segmentation, the criteria for placement of systems in these zones, and rules governing communications between the zones.

3 Scope

This standard applies to all networks and systems managed by RXO, Inc. including its subsidiaries, divisions, and any other entities (collectively, "RXO") and any other system that connects to an RXO managed network. Networks and systems that can not comply with these standards require an exception from the Global Security Office.

4 Network Segmentation Standard

Network Zones

The following network zones must be used to segment systems at each site. Each zone may be one or more VLANs. Not all sites will require all zones. Zones must be fully documented.

- **Internet Zone (DMZ)** – This is a low trust zone. All systems that require direct connectivity from the internet must reside in this zone. Systems in this zone are the most vulnerable to cyber-attacks. The Internet DMZ should be implemented as a Layer 3 subnet. Systems in this zone include internet facing web servers, load balancers, etc.
- **Internet Support Zone** – This is a medium trust zone. This zone supports the low trust Internet DMZ. The systems in this zone require connectivity to systems in the Internet DMZ. Untrusted users may access or provide information to these systems. The systems in this zone provide middleware and backend support for systems in the Internet DMZ.
- **Remote Access Zone** – This zone will house the VPN concentrators and may allow access to other zones and applications only as required to perform job duties.
- **Infrastructure Zone** – This zone contains servers and appliances providing common infrastructure services such as DHCP, NTP, Domain Controllers, and DNS.
- **Management Zone** – This zone contains servers used to manage the IT environment. This includes SCCM, SolarWinds, etc.
- **Security Zone** – This zone contains all systems providing security services to the IT Environment (Security Protection Assets), including Cylance, Encase, Tanium, and Splunk, etc.
- **Controller Zone** – This zone contains systems that are owned, managed, or operated by 3rd parties. Systems in this zone may be “black box” or have reduced functionality operating systems that may be more susceptible to security vulnerabilities or can’t be patched due to vendor support restrictions.
- **Server Zone** – This zone contains servers providing application services.
- **Development Zone** – This zone contains servers used to development of applications. Development servers should be separated from production servers.
- **VoIP Zone** – This zone contains VoIP phones and phone systems.
- **User Zone** – This zone is comprised of all end-user compute devices such as desktops, laptops, iPads, printers, etc.
- **Guest Access Zone** – This zone should be utilized to provide Internet access for guests at company locations.
- **Geographical Zones** – These zones should be utilized to provide or restrict access for certain specified countries or other geographical areas. Specific zones to be created include North America, Europe, China, India, and one or more zones for designated countries to be blocked, such as Russia, North Korea, and Iran.
- **Customer-specific zones** that isolate customer devoted systems and data on their own logical network may also be defined, as required by contract. As example, a government contract having Controlled Unclassified Information (CUI) may drive a requirement for a CUI zone. Access Controls for these zones may be customized to comply with customer contracts but must provide access from the Security, Infrastructure and Management Zones.

Security Levels

100-71: Trusted

Internal (Security Level 100)

- RXO Inc. networks where users and internal services reside
- This Zone incorporates- Production, Internal, End-users, Management Zone, Security Zones, and includes North America and Europe

Isolated (Security level 60)

- RXO networks where QA, development, and lab devices reside
- This Zone incorporates- QA servers, Developers servers and DR-Test Zone, and includes India

Secure (Security level 55)

- Network between Trusted and DMZ
- This Zone incorporates- Common, Infrastructure Zones.

70-31: Risky

DMZ (Security level 50)

- RXO controlled networks that are connected to external networks.
- This Zone incorporates- DMZ servers.

Third Party (Security level 30)

- IP addresses, and/or devices belonging to a Third Party with a dedicated connection
- This Zone incorporates- Third party hosted appliances and services, and includes China.

30-0: Untrusted

Guest Access (Security level 10)

- RXO Networks for guests to access internet services

Internet (Security level 5)

- All Public IP addresses not assigned to RXO or an RXO Third Party partner

Access blocked (Security level 0)

- All IP addresses in Russia, North Korea, Iran, Cuba, Syria, Sudan, and any other Government-mandated country.

Inter-zone Communication and Access Controls

The security value of network segmentation is derived from limiting network communications between zones to only that necessary to provide IT services and manage the IT environment. Unless otherwise proscribed in this standard, communication between zones is not permitted. All approved communications between zones must be documented in Access Control Lists (ACLs).

Any connectivity from the Internet must terminate in the Internet Zone (DMZ). No other zones may accept external connections. This includes administrative protocols such as SSH or Telnet.

Systems in the Internet Zone may access specific systems in the Internet Support Zone as required to support system functions. Systems in the Internet Support Zone may not access systems in the Internet Zone.

The Infrastructure Zone may access the Internet Zone (DMZ), and vice versa, only to the extent required to support the delivery of infrastructure services that rely on Internet connectivity such as DNS and NTP. This zone interaction must be limited to the protocols, ports, and devices required to support the service.

The Security and Management Zones may access systems in all other zones as required. Other zones may not access the Security and Management Zones.

All zones may access the Infrastructure Zone only as needed to provide infrastructure services to those zones.

The VoIP zone must not have access to other zones except as needed to receive infrastructure or other services required to run VoIP devices.

The User Zone may access:

- The Internet Zone only as required for internet proxy services.
- The Infrastructure Zone only as required to receive infrastructure services.
- The Server Zone only as required to access internal services.
- The Security and Management Zones only as required to support the systems and services in these zones. Access to these zones must be provided via "jump" servers and only to authorized personnel.

The Guest Access Zone is provided to allow visitors to RXO access to the Internet, and as such may access the Internet Zone only as required for internet proxy services. The Guest Access Zone may not access any internal zones except as needed to receive infrastructure or other services required to run.

<u>Severity</u>	<u>Business Requirement</u>	<u>Action</u>
Critical	All traffic from Internet to Trusted, Secure, Isolated, or Third Party	Security exception required for approval with business justification
	All traffic into or out from Guest Access zone (except Guest to Internet using web or VPN ports)	Exception rule will be active for defined time frame
High	Source or destination of "any" in or out of Secure, Isolated, DMZ, or Third Party	Exception will Required to be approved by Information Security
	All traffic from Internet to DMZ	Exception rule will be active for pre-defined time frame.
	Traffic that is from DMZ or Third Party to DMZ or Third Party	Policy will need to be removed after the pre-defined time.
	Any rule unused for 180 days will require renewal with business justification.	
Medium	Source or destination of "any" in or out of the Internal Zone	Business as usual, this denotes highly permissive rules
	All traffic from DMZ to Internal and Internet to DMZ	Provides a warning for unused rules before the 365-day limit
	Any rule unused for 240 days	
Low	All the Traffic flowing through internally will require an ACI security policy guideline	Business as usual, this is used to notify security of rules that require review
	All traffic into or out from Guest Access zone (except Guest to Internet)	
	Inter-zone traffic with source or destination of "any"	

Site-to-Site Communications

Site to site and site to datacenter communications are not permitted unless required to support business or IT processes. In such cases a valid business justification must be provided to the GSO for each connection. The connection must be limited to the protocols, ports, and devices required to support the process.

External Access to Systems

External access to network zones must be provided through the corporate VPN solution using multi-factor authentication. VPN profiles must be configured to only allow users access to the zones, applications, tools, and systems they require to perform job duties. Only authorized administrative and support personnel may access "jump" servers and only when necessary to perform their job duties.

Internal Network Safeguards

- Ensure that each of RXO's endpoint computing systems' Virtual Local Area Networks (VLANs) enforces privatization to prevent computing systems from communicating with other systems on the same VLAN.
- Maintain network authentication systems (802.1x) for RXO's wired network.
- Ensure that RXO's network authentication systems (802.1x) for each of its wired networks require certificate-based authentication.
- Maintain network authentication systems (802.1x) for RXO's wireless network.
- Ensure that RXO's network authentication systems (802.1x) for each of its wireless networks require certificate-based authentication.
- Ensure RXO's network authentication systems (802.1x) for each of RXO's wireless networks follow the RXO Cryptography policy to encrypt all wireless connections.
- Ensure RXO's network authentication systems (802.1x) for each of RXO's wired or wireless networks require defined, documented health checks of computing systems prior to allowing them access to the network.

Certificate of Review

Network Segmentation Standard

July 2nd 2026 2:09:48 pm

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Tuesday, April 14, 2026 2:20 PM EDT
Faisal Khan		Policy Approver	Approved	Tuesday, June 30, 2026 12:27 PM EDT
Mark Gutman		Policy Admin	Published	Thursday, July 2, 2026 2:09 PM EDT