



Secure Server Standard

DOC-IT-IS-29
Revision 2.0
FEBRUARY 18, 2026

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	11/01/2025	Initial Version
2.0	2/18/2026	Additional requirements & CIS references added

29 Table of Contents

29 Secure Server Standard	4
29.1 Executive Summary	4
29.2 Purpose	4
29.3 Scope	4
29.4 Secure Server Standards Statement.....	5
29.4.1 Maintain Asset Inventory & Ownership	5
29.4.2 Secure the Operating System	5
29.4.3 Secure the Server Software	5
29.4.4 Maintain the Security of the Server	6
29.5 Responsibilities	8
29.5.1 InfoSec	8
29.5.2 Server Administrators.....	8
29.5.3 Vulnerability Management.....	8
29.5.4 SOC Team	8
29.6 Compliance	8
29.7 Exceptions.....	9
29.8 Review and Updates	9
29.9 References	9
29.10 Definitions.....	10

29 Secure Server Standard

29.1 Executive Summary

This document outlines RXO's Secure Server Standard, designed to ensure the confidentiality, integrity, and availability of RXO's server infrastructure, to reduce attack surface, prevent unauthorized software, enforce secure configuration, and ensure timely vulnerability remediation and audit visibility. It defines approved secure ports, encryption requirements, monitoring protocols, and vulnerability management practices. The standard aligns with industry frameworks such as ISO/IEC 27001, NIST SP 800-53, and CIS Controls, which include a prioritized set of safeguards designed to defend against common cyberattacks.

29.2 Purpose

The purpose of this document is to define standards for the secure server configuration and management of network ports at RXO. This includes enforcing encrypted communication, minimizing exposure to cyber threats, and maintaining compliance with industry best practices. This standard defines enforceable security requirements for:

- Secure configuration baselines for servers
- Prohibition of unnecessary software (including web browsers)
- Continuous vulnerability management
- Centralized logging and monitoring
- Controlled exceptions with compensating controls and risk acceptance

29.3 Scope

This standard applies to 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.

This standard applies to all server assets (physical, virtual, cloud-hosted, managed service environments) across production and non-production environments, including but not limited to:

- Windows and Linux servers
- Domain controllers and directory infrastructure
- Application and database servers
- Bastion hosts / jump servers
- Container hosts and orchestration worker nodes

29.4 Secure Server Standards Statement

29.4.1 Maintain Asset Inventory & Ownership

- All servers **MUST** be registered in the RXO Asset Inventory following the RXO Asset Management Policy with at least the following information:
 - Asset owner
 - Environment classification (production, non-production, etc.)
 - Criticality
- Reference CIS Control 1, actively managing assets and identifying unauthorized and unmanaged assets.

29.4.2 Secure the Operating System

Secure Configuration Baselines / Hardening

- Servers **MUST** be built using the latest secure baseline from company-approved images aligned to relevant CIS Benchmarks (Level 1 minimum; Level 2 for higher-risk tiers where feasible).
- Servers **MUST** be secured following the RXO Operations Security Policy, the RXO Access Control Policy, and the RXO Password Management Standard.
- Reference CIS Control 4, which requires organizations to “establish and maintain secure configuration of enterprise assets (including servers) and software.

Identity, Privilege, and Administrative Access

- Administrative access **MUST** follow least privilege and separation of duties:
 - Use dedicated admin accounts for privileged work.
 - Restrict and monitor privileged group membership.
- Local administrator access **MUST** be controlled and minimized.
- Service accounts **MUST** be unique per function and restricted to only required privileges (no interactive logon unless explicitly required and approved).

29.4.3 Secure the Server Software

Software Inventory, Authorization, and Prohibited Software

- Servers **MUST** run only Information Security approved, business-justified software required for the server’s role.
- Servers **MUST** enforce a process to detect and address unauthorized software (e.g., inventory tooling + removal workflow).
- Web browsers are prohibited on all servers by default (including, but not limited to, Chrome/Edge/Firefox or equivalents). This is an explicit “least functionality” and attack surface reduction measure consistent with secure configuration expectations.
 - Rationale: browsers are frequent targets for critical vulnerabilities and enable direct interaction with untrusted web content. Internal vulnerability evidence has shown

severe Chrome vulnerabilities present on server-class assets, demonstrating real exposure when browsers exist on servers.

- Any need for prohibited software (including browsers) **MUST** go through the Security Exception process (see Section 29.7).
- Unauthorized software discovered on servers will be removed as part of standard security remediation, especially when it increases attack surface or introduces exploitable vulnerabilities.
- Reference CIS Control 2, which requires that organizations actively manage software so only authorized software is installed and can execute, and unauthorized software is prevented or removed.

Services Management

- All unused services, packages and features **MUST** be disabled or uninstalled on all servers.

Encryption Enforcement

- All services exposed via open ports **MUST** use secure protocols (e.g., TLS 1.2 or higher) configured in accordance with the RXO Cryptography Policy.
- Unencrypted protocols (e.g., Telnet, FTP, HTTP) are prohibited.

Server Resource Constraints

- Install server content on a different hard drive or logical partition than the OS and server software.
- Place a limit on the amount of hard drive or partition space that is dedicated to uploads, if uploads to the server are allowed. Ideally, uploads should be placed on a separate partition to provide stronger assurance that the hard drive limit cannot be exceeded.
- Ensure log files are stored in a location that is sized appropriately. Ideally log files should be stored on a separate partition.
- Configure an appropriate maximum number of server processes and network connections that the server should allow.

29.4.4 Maintain the Security of the Server

Network Exposure Reduction & Port Management

- Servers **MUST** only expose required ports/services (“deny-by-default” posture).
 - Unused ports and protocols **MUST** be disabled on all systems and devices.
 - RXO has defined a list of approved secure ports for use in its environments. These ports are configured with strict access controls, encryption requirements, and

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

- Port security **MUST** be implemented on switches to prevent unauthorized device connections.
- Administrative protocols **MUST** be restricted to authorized management networks and controlled access paths.
- Access **MUST** be restricted using firewalls, ACLs, and network segmentation.
- Internet exposure **MUST** be explicitly approved and documented through the exception process.

Audit Logging, Time Sync and Monitoring

- Servers **MUST** generate audit logs for security-relevant events (authentication, privilege changes, policy/config changes, service starts/stops where relevant).
- All port activity **MUST** be logged and monitored via the company Security Information and Event Management (SIEM) system and in accordance with the RXO Information Logging & Monitoring Standard and the RXO Audit & Accountability Policy.
- Logs **MUST** be forwarded to the RXO centralized logging platform/SIEM and protected from tampering.
- Logs **MUST** be retained per enterprise retention requirements; higher criticality systems may require longer retention.
- Alerts **MUST** be generated for unauthorized scans, traffic anomalies, or configuration changes.
- Time synchronization **MUST** be standardized across servers (for correlation and incident response).
- Reference CIS Control 8, which reflects CIS log management expectations for collection/review/retention, and requires organizations to “collect, alert, review, and retain audit logs” to detect, understand, and recover from attacks.

Continuous Vulnerability Management & Patching

- Conduct regular scans to identify open ports and assess risks in accordance with the RXO Vulnerability Management Standard.
- Remediate findings within 30 days or submit a risk acceptance form to the BISO.
- Reference CIS Control 7, which requires a plan to continuously assess and track vulnerabilities to remediate and minimize attacker opportunity windows.

Data Protection, Backup and Recovery

- Ensure the server is configured to comply with the RXO Disaster Recovery and Business Continuity Policy.

- Sensitive data on servers **MUST** be protected using approved encryption mechanisms where applicable.
- Servers **MUST** be included in backup and recovery processes appropriate to criticality.
- Recovery procedures **SHOULD** be tested periodically for critical systems.

29.5 Responsibilities

29.5.1 InfoSec

- Owns this standard, defines risk thresholds, reviews exceptions, and validates compensating controls.
- Ensure the implementation and compliance with this standard across all servers.
- Conduct regular audits of server configurations.
- Maintains mappings to CIS Controls.

29.5.2 Server Administrators

- Ensure configuration on all servers complies with this standard and with the RXO Disaster Recovery and Business Continuity Policy.
- Notify the IT security team of any issues or breaches involving servers.
- Remediate findings within required timelines.

29.5.3 Vulnerability Management

- Operate scanning/assessment cadence and track remediation per defined SLAs (risk-based) and the RXO Vulnerability Management Standard.

29.5.4 SOC Team

- Ensure collection, retention, and alerting on required logs.

29.6 Compliance

Non-compliance with this policy may result in access restrictions to affected systems or disciplinary actions as per RXO's guidelines. Systems found out of compliance **MUST** be remediated within the defined SLA or placed under an approved exception. Unauthorized software, including prohibited browser installations, will be removed as part of standard remediation to reduce risk exposure.

Compliance with this standard is measured through:

- Configuration baseline compliance (benchmark/baseline checks)
- Vulnerability scan results and remediation timeliness
- Software inventory and unauthorized software detection/removal

- Logging coverage and retention validation

Managers/owners must address non-compliance and implement corrective actions consistent with broader compliance expectations in internal security compliance policy language.

29.7 Exceptions

Any exceptions to this policy must be approved in writing prior to implementation by the RXO Governance Risk and Compliance (GRC) team and must include:

- A valid business justification and scope (systems and environments).
- Compensating controls.
- Expected duration or expiration date.
- Residual risk acceptance by the appropriate authority.

Examples requiring exceptions include:

- Installing a web browser on a server.
- Running unsupported/EOL software.
- Deviations from CIS Benchmark baseline settings on high-impact controls.

29.8 Review and Updates

This standard will be reviewed annually, or upon major infrastructure or threat landscape changes, or as required due to changes in business or technical requirements.

29.9 References

- NIST 800-123: Guide to General Server Security
- RXO Asset Management Policy
- RXO Operations Security Policy
- RXO Access Control Policy
- RXO Password Management Standard
- RXO Cryptography Policy
- RXO Information Logging & Monitoring Standard
- RXO Vulnerability Management Standard
- RXO Disaster Recovery and Business Continuity Policy
- RXO Cloud Security Standard

- ISO/IEC 27001
- CIS Controls v8/v8.1 overview (prioritized safeguards)
- CIS Benchmarks overview (secure configuration guidelines mapped to CIS Controls)

29.10 Definitions

- **Server:** Any compute instance providing services/workloads (physical/virtual/cloud).
- **Secure Baseline:** An approved hardened configuration aligned to CIS Benchmarks or enterprise hardening standards.
- **Unauthorized Software:** Software not explicitly approved for the server role/owner and not documented in the authorized software inventory.
- **Exception:** Time-bound, approved deviation with compensating controls and risk acceptance.
- **CIS:** Center for Internet Security.

Certificate of Review

Secure Server Standard

March 24th 2026 12:10:20 pm

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Wednesday, February 18, 2026 3:29 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, March 24, 2026 11:02 AM EDT
Mark Gutman		Policy Admin	Published	Tuesday, March 24, 2026 12:10 PM EDT