



Audit & Accountability Policy

DOC-IT-IS-AU-01
Revision 1.0
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	11/01/2025	Initial Version

Table of Contents

1.0. Executive Summary	4
2.0. Purpose	4
3.0. Scope	4
4.0. Roles & Responsibilities	5
4.1 Information Security.....	5
4.2 Identity & Access Management	5
4.3 Server Administration Team(s)	5
5.0. Compliance	6
5.1 Compliance Measurement.....	6
5.2 Exceptions	6
5.3 Non-Compliance.....	6
6.0. Audit & Accountability Policy Requirements	7
6.1 System Auditing	7
6.2 User Accountability	7
6.3 Event Review.....	7
6.4 Audit Failure Alerting	8
6.5 Audit Correlation.....	8
6.6 Reduction & Reporting	8
6.7 Authoritative Time Source.....	8
6.8 Audit Protection	9
6.9 Audit Management	9
7.0 Related Polices, Standards & Processes	10
7.1 Related Company Policies & Standards.....	10
7.2 Related Industry Best Practices, Policies & Standards	10
8.0 Definitions & Terms	10

1.0. Executive Summary

Audits are independent reviews and examinations to assess the adequacy of information system controls and to ensure that all policies and standards are being followed. Accountability is the principle that a user is trusted to safeguard and control information and must answer to the proper authority for the loss or misuse of the information.

2.0. Purpose

The purpose of this Policy is to establish the Audit & Accountability requirements governing the practices and processes incorporated within RXO's Cybersecurity Program and Secure Computing Environment implemented for storing, processing, and transmitting sensitive company and customer data. This Policy is intended to outline Audit & Accountability Best Practices and the Minimum Standard for protecting RXO and customer data, and the systems which store, process, and transmit data within RXO's system boundaries.

3.0. Scope

The Audit & Accountability Policy covers all RXO information and information system assets that are within scope of RXO's environment. This includes all assets which store, process, and transmit RXO company and customer data, and assets which provide security protection for securing company assets.

This Policy applies to all RXO subsidiaries, divisions, and operating entities, all employees, contractors, and third-party partners, as well as all data and systems used for supporting business functions within scope of RXO's business units, in pursuit of protecting data.

4.0. Roles & Responsibilities

4.1 Information Security

- 4.1.1 Establish and maintain a capability to create and retain information system audit logs and records to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
- 4.1.2 Maintain information system practice documents detailing the tools/utilities that provide audit record generation.
- 4.1.3 Determine which events are to be recorded and logged appropriately.
- 4.1.4 Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events.
- 4.1.5 Review logged events.
- 4.1.6 Receive alerts in the event of audit logging failures.
- 4.1.7 Correlate audit record review, analysis, and reporting for investigation and response to indications of unlawful, unauthorized, or suspicious activity.
- 4.1.8 Review reports of audit findings.
- 4.1.9 Identify and determine access permissions to audit logging information and audit logging functions.
- 4.1.10 Limit management of audit logging functionality to a subset of authorized, privileged users.
- 4.1.11 Authorize access to privilege users who have access to audit information and audit logging tools.
- 4.1.12 Ensure the information system supports on-demand (continuous) audit review, analysis, and reporting requirements.
- 4.1.13 Manage and maintain a capability for providing on-demand audit review, analysis, and reporting.
- 4.1.14 Ensure audit information and audit logging tools are protected from unauthorized access, modification, deletion, etc.
- 4.1.15 Ensure the information system has a capability to compare and synchronize internal system clocks with an authoritative time source to generate accurate time stamps for audit records.

4.2 Identity & Access Management

- 4.2.1 Ensure the information system has a capability to compare and synchronize internal system clocks with an authoritative time source to generate accurate time stamps for audit records.
- 4.2.2 Manage and maintain the capability that compares and synchronizes internal system clocks with an authoritative time source.

4.3 Server Administration Team(s)

- 4.3.1 Manage audit record storage capacity and configure capacity & auditing to prevent such capacity being exceeded.
- 4.3.2 Work with GSO to ensure logs are sent to the central logging server.

5.0. Compliance

5.1 Compliance Measurement

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs and interviews, business tool reports, internal and external audits, and feedback to the standards owner(s).

5.2 Exceptions

Any exception to the policy must be approved by the InfoSec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Security assessments are a requirement of the change control process, and all asset owners are required to adhere to this policy unless found to be exempt. All system releases must pass through the change control process. Any assets that do not adhere to this standard may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

6.0. Audit & Accountability Policy Requirements

6.1 System Auditing

Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

RXO must define the necessary audit logs to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. Audit logs which are created must contain the defined content and the necessary retention requirements must be applied.

- a) RXO must specify which audit logs are necessary to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
- b) RXO must define the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
- c) RXO must ensure audit records are created (generated).
- d) RXO must verify audit records contain the defined content once created.
- e) RXO must define the retention requirements for audit records.
- f) RXO must ensure audit records are retained as defined.

6.2 User Accountability

Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

RXO must define the content of the audit records needed to support the ability to uniquely trace users to their actions.

- a) RXO must define the content of audit records needed to support the ability to uniquely trace users to their actions.
- b) RXO must ensure that audit records contain the defined content once created.

6.3 Event Review

Review and update logged events.

RXO must define a process for determining when to review logged events and must update event types being logged based on the review.

- a) RXO must define a process for determining when to review logged events, no less than annually.
- b) RXO must ensure the event types being logged are reviewed in accordance with the defined review process.
- c) RXO must ensure the event types being logged are updated based on the review.

6.4 Audit Failure Alerting

Alert in the event of an audit logging process failure.

RXO must define the different types of audit logging process failures which generate alerts. Personnel or roles to be alerted in the event of an audit logging process failure must be identified.

- a) RXO must identify the personnel or roles to be alerted in the event of an audit logging process failure.
- b) RXO must define types of audit logging process failures for which an alert must be generated.
- c) RXO must ensure the identified personnel or roles are alerted in the event of an audit logging process failure.

6.5 Audit Correlation

Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

RXO must define and correlate the audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

- a) RXO must define the audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
- b) RXO must ensure that the defined audit record review, analysis, and reporting processes are correlated.

6.6 Reduction & Reporting

Provide audit record reduction and report generation to support on-demand analysis and reporting.

RXO must provide an audit record reduction capability that supports on-demand analysis and on-demand report generation capabilities.

- a) RXO must determine if an audit record reduction capability that supports on-demand analysis is provided.
- b) RXO must ensure a report generation capability that supports on-demand reporting is provided.

6.7 Authoritative Time Source

Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

RXO must specify an authoritative source with which to compare and synchronize internal system clocks. Internal system clocks must be used to generate time stamps for audit records and must be synchronized with the specific authoritative time source.

- a) RXO must leverage internal system clocks to generate time stamps for audit records.
- b) RXO must specify an authoritative source with which to compare and synchronize internal system clocks.
- c) RXO must ensure internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.

6.8 Audit Protection

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

RXO must protect audit information and logging tools from unauthorized access, modification, and/or deletion.

- a) RXO must protect audit information from unauthorized access.
- b) RXO must protect audit information from unauthorized modification.
- c) RXO must protect audit information from unauthorized deletion.
- d) RXO must ensure audit logging tools are protected from unauthorized access.
- e) RXO must ensure audit logging tools are protected from unauthorized modification.
- f) RXO must ensure audit logging tools are protected from unauthorized deletion.

6.9 Audit Management

Limit management of audit logging functionality to a subset of privileged users.

RXO must define and limit access to manage audit logging functionality to a subset of defined privileged users.

- a) RXO must define a subset of privileged users granted access to manage audit logging functionality.
- b) RXO must ensure that the management of audit logging functionality is limited to the defined subset of privileged users.

7.0 Related Policies, Standards & Processes

Detailed processes and procedures must be written to implement the standards in this document.

7.1 Related Company Policies & Standards

These policies and standards can be found on the GSO Security Policies and Standards SharePoint site.

- 7.1.1 Asset Management Policy
- 7.1.2 Access Control Policy
- 7.1.3 Information Classification Standard
- 7.1.4 Information Logging & Monitoring Standard
- 7.1.5 Security Incident Response Policy
- 7.1.6 IT Asset Disposal Standard
- 7.1.7 Cryptography Policy

7.2 Related Industry Best Practices, Policies & Standards

- 7.2.1 [NIST SP 800-92 - Guide to Computer Security Log Management](#)
- 7.2.2 [NIST SP 800-171](#)
- 7.2.3 Sarbanes-Oxley Act (SOX) of 2002
- 7.2.4 [OWASP C9: Implement Security Logging and Monitoring](#)

8.0 Definitions & Terms

OWASP	Open Web Application Security Project
NIST	National Institute of Standards & Technology
SOX	Sarbanes-Oxley Act of 2002
GSO	RXO's Global Security Office

Certificate of Review

Audit and Accountability Policy

March 24th 2026 12:10:00 pm

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Thursday, January 8, 2026 1:19 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, March 24, 2026 11:07 AM EDT
Mark Gutman		Policy Admin	Published	Tuesday, March 24, 2026 12:10 PM EDT