



Information Logging & Monitoring Standard

DOC-IT-IS-24
Revision 1.0
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	11/01/2025	Initial Version

Table of Contents

24.0. INFORMATION LOGGING & MONITORING STANDARD4

24.1. EXECUTIVE SUMMARY4

24.2. PURPOSE.....4

24.3. SCOPE.....4

24.4. ROLES & RESPONSIBILITIES5

 24.4.1 APPLICATION OWNERS.....5

 24.4.2 SERVER / PLATFORM OWNERS5

 24.4.3 NETWORK MANAGEMENT TEAM.....5

 24.4.4 VULNERABILITY MANAGEMENT TEAM5

 24.4.5 INFOSEC TEAM.....5

24.5. COMPLIANCE6

 24.5.1 COMPLIANCE MEASUREMENT6

 24.5.2 EXCEPTIONS6

 24.5.3 NON-COMPLIANCE6

24.6. STANDARDS6

 24.6.1 ASSET MANAGEMENT6

 24.6.2 ACCESS CONTROL6

 24.6.3 GENERAL INFORMATION LOGGING REQUIREMENTS.....6

 24.6.4 ACTIVITIES TO BE LOGGED.....7

 24.6.5 LOG ELEMENTS8

 24.6.6 FORMATTING.....8

 24.6.7 TRANSMISSION.....8

 24.6.8 STORAGE.....8

 24.6.9 MONITORING & ANALYSIS.....9

24.7. RELATED POLICES, STANDARDS & PROCESSES10

 24.7.1 RELATED COMPANY POLICIES & STANDARDS10

 24.7.2 RELATED INDUSTRY BEST PRACTICES, POLICIES & STANDARDS10

24.8. DEFINITIONS & TERMS11

24.0. Information Logging & Monitoring Standard

24.1. Executive Summary

Logging is a concept that most developers already use for debugging and diagnostic purposes. Security logging is an equally basic concept: to log security information during the runtime operation of an application. Monitoring is the live review of application and security logs using various forms of automation. The same tools and patterns can be used for operations, debugging and security purposes.

The amount of information logged must be sufficient to support analysis and response, but should not include private, confidential, or sensitive information. Information logged should be regularly reviewed to ensure the organization is not logging too much or too little information.

24.2. Purpose

The purpose of this document is to define the information logging & monitoring standards within RXO. Logging is used to feed intrusion detection systems, for forensic analysis and investigations, and to satisfy regulatory and compliance requirements.

These standards will limit the attack surface of RXO' applications available both internally and externally, protect customers' sensitive data, and satisfy compliance with any relevant policies in place.

24.3. Scope

This standard applies to RXO, Inc., including all subsidiaries, divisions, and operating entities. All directors, officers, full-time and part-time employees, agents, contractors, and third parties acting on behalf of RXO must comply with this policy.

This standard covers all network devices, servers, workstations, and internal and external applications used by any group, department, or other application developed or used by RXO, including all of its business units, to store, process or otherwise manage customer data or sensitive company data.

All asset owners, including those of cloud-based or third-party applications, are responsible for taking the appropriate steps to follow these security logging best practices.

Assets, systems, or applications that cannot comply with these standards require an exception from the Infosec team.

24.4. Roles & Responsibilities

24.4.1 Application Owners

- 24.4.1.1 Application owners must document the information available in their logs, and what information will be sent to the central logging server.
- 24.4.1.2 Documentation should also be provided to the Incident Response Team to ensure they are aware of any new potential threat surfaces.
- 24.4.1.3 All application owners must ensure logging information is sent to the central logging system to meet all requirements of the Company Information Logging & Monitoring Standard.

24.4.2 Server / Platform Owners

- 24.4.2.1 Server / platform owners must document the information available in their logs, and what information will be sent to the central logging server.
- 24.4.2.2 Documentation should also be provided to the Incident Response Team to ensure they are aware of any new potential threat surfaces.
- 24.4.2.3 All server / platform owners must ensure logging information is sent to the central logging system to meet all requirements of the Company Information Logging & Monitoring Standard.

24.4.3 Network Management Team

- 24.4.3.1 Network device owners must document the information available in their logs, and what information will be sent to the central logging server.
- 24.4.3.2 Documentation should also be provided to the Incident Response Team to ensure they are aware of any new potential threat surfaces.
- 24.4.3.3 All network device owners must ensure logging information is sent to the central logging system to meet all requirements of the Company Information Logging & Monitoring Standard.

24.4.4 Vulnerability Management Team

- 24.4.4.1 Vulnerability Management Team must document the information available in their logs, and what information will be sent to the central logging server.
- 24.4.4.2 Documentation should also be provided to the Incident Response Team to ensure they are aware of any new potential threat surfaces.
- 24.4.4.3 Vulnerability Management Team must ensure logging information is sent to the central logging system to meet all requirements of the Company Information Logging & Monitoring Standard.

24.4.5 InfoSec Team

- 24.4.5.1 The InfoSec team will conduct security assessments of any new or updated assets to review the information logging and monitoring controls.
- 24.4.5.2 The InfoSec team will update this Standard for any new or changed requirements regarding information to be sent to the central logging server in audit records.

24.5. Compliance

24.5.1 Compliance Measurement

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

24.5.2 Exceptions

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

24.5.3 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.

24.6. Standards

24.6.1 Asset Management

- 24.6.1.1 All assets, with their version control information, must be fully documented and added to the company Asset Inventory, including those for internal, external, and cloud-based systems.
- 24.6.1.2 The company Asset Management Policy will apply to all assets, including internal, external, and cloud-based systems.
- 24.6.1.3 All assets will follow the Information Logging and Monitoring standards contained in this document.

24.6.2 Access Control

- 24.6.2.1 The company Access Control Policy will apply to all information logging and monitoring tools used.
- 24.6.2.2 Access control policies for logs and logging and monitoring tools must separate administrative functions from user functions.
 - 24.6.2.2.1 A subset of privileged users who will be granted access to manage audit logging functionality must be defined and access limited to those users.
- 24.6.2.3 Access control policies must protect audit tools from unauthorized access, modification, and deletion.
- 24.6.2.4 Access control policies must protect audit information from unauthorized access, modification, and deletion.

24.6.3 General Information Logging Requirements

- 24.6.3.1 All logging data must be collected and sent to the central logging system or security information and event management (SIEM) system.

- 24.6.3.2 The audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity must be defined and documented.
- 24.6.3.3 The content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity must be defined and documented for each asset.
- 24.6.3.4 The content of the audit records must support the ability to uniquely trace users to their actions, including dates and times of those actions.
- 24.6.3.5 Internal system clocks should be used to generate date/time stamps for audit records.
- 24.6.3.5.1 An authoritative source with which to compare and synchronize internal system clocks must be used.
- 24.6.3.5.2 Internal system clocks used to generate time stamps for audit records should be regularly compared to and synchronized with the specified authoritative time source.
- 24.6.3.6 The retention requirements for all audit records must be defined and documented but must be at a minimum 1 year.
- 24.6.3.6.1 In 2020, the average time to identify, analyze and contain a breach, as reported by IBM, was 280 days.

24.6.4 Activities to be Logged

At a minimum, log records shall be created whenever any of the following activities are requested to be performed by the system:

- 24.6.4.1 Create, read, update, or delete confidential or sensitive information, including confidential authentication information such as passwords (taking care NOT to log the actual password or other confidential/sensitive information).
- 24.6.4.2 Create, update, or delete other information (such as any deletion of a file).
- 24.6.4.3 Initiate a network connection.
- 24.6.4.4 Accept a network connection.
- 24.6.4.5 User authentication and authorization activities, such as user login and logout, failed logins, successful login after previously failing, an account being locked after max retries, password change failures.
- 24.6.4.6 When a token is created, revoked, deleted, attempted re-use of a previously revoked token.
- 24.6.4.7 Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes.
- 24.6.4.8 System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes.
- 24.6.4.9 Application process startup, shutdown, or restart.
- 24.6.4.10 Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault.
- 24.6.4.11 Requests that violate server-side access control rules.
- 24.6.4.12 All activity by privileged users such as admin should be recorded.
- 24.6.4.13 Enabling or disabling of any system monitoring resources.
- 24.6.4.14 Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

24.6.5 Log Elements

Log records shall identify or contain at least the following elements:

- 24.6.5.1 Type of action – examples include authorize, create, read, update, delete, and accept network connection.
- 24.6.5.2 Subsystem performing the action – examples include process or transaction name, process, or transaction identifier.
- 24.6.5.3 Identifiers (as many as available) for the subject requesting the action – examples include username, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- 24.6.5.4 Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- 24.6.5.5 Before and after values when action involves updating a data element, if feasible.
- 24.6.5.6 Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
- 24.6.5.7 Whether the action was allowed or denied by access-control mechanisms.
- 24.6.5.8 Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.
- 24.6.5.9 A severity value.

24.6.6 Formatting

- 24.6.6.1 Wherever possible, follow a common logging format and approach within the system and across systems of the organization.
 - 24.6.6.1.1 An example of a common logging framework is the Apache Logging Services which helps provide logging consistency between Java, PHP, .NET, and C++ applications.
- 24.6.6.2 To facilitate analysis of logs, implement automated methods of converting logs with different content and formats to a single standard format with consistent data field representations.
- 24.6.6.3 Where possible, use event aggregation, where similar entries are consolidated into a single entry containing a count of the number of occurrences of the event.

24.6.7 Transmission

- 24.6.7.1 A reliable connection method must be used to ensure delivery of information to the central logging server, such as TCP.
- 24.6.7.2 The use of a secure protocol to protect the confidentiality of transmitted log messages is recommended, such as the latest Transport Layer Security (TLS) or Secure Shell tunnel (SSH) versions to avoid the use of the weakest cipher suites.
- 24.6.7.3 The Company Cryptography Policy should be followed to ensure proper transmission integrity protection and authentication.

24.6.8 Storage

- 24.6.8.1 Logs must be stored in such a way as to protect their confidentiality and integrity, preferably using FIPS-validated encryption, and following the Company Cryptography Policy.
- 24.6.8.2 Log rotation and archiving rules must be defined and documented.
- 24.6.8.3 Log preservation rules, such as in the case of a detected intrusion or breach, must be defined and documented.

- 24.6.8.4 Rules for clearing or disposal of logs must be defined and documented and must follow the Company IT Asset Disposal Standard.

24.6.9 Monitoring & Analysis

- 24.6.9.1 Alerts must be generated in the event of an audit log process failure.
- 24.6.9.1.1 Personnel or roles to be alerted in the event of an audit logging process failure must be identified and documented.
- 24.6.9.1.2 The types of audit logging process failures for which alert will be generated must be defined.
- 24.6.9.2 A report generation capability that supports on-demand reporting must be provided.
- 24.6.9.2.1 An audit record reduction capability that supports on-demand analysis should be provided.
- 24.6.9.2.2 A reporting tool that supports event aggregation, where event aggregation, similar entries are consolidated into a single entry containing a count of the number of occurrences of the event, is preferred.
- 24.6.9.3 A process of audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity must be defined.
- 24.6.9.3.1 The frequency of the reviews must be defined.
- 24.6.9.3.2 Run-time alerts for significant events should be defined and implemented.
- 24.6.9.4 A process to review and update logged events must be defined.
- 24.6.9.4.1 The frequency of the reviews must be defined.
- 24.6.9.4.2 The event types being logged must be reviewed.
- 24.6.9.4.3 Based upon the reviews, an update of the event types being logged should be considered, findings documented, and other appropriate documentation updated accordingly.
- 24.6.9.5 The Company Security Incident Response procedures should be updated to include information logging security incidents, indicators, and responses (as example, deletion of a log file), as well as critical audit record types that requiring alerting, investigation, and response.

24.7. Related Policies, Standards & Processes

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

24.7.1 Related Company Policies & Standards

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

- 24.7.1.1 Asset Management Policy
- 24.7.1.2 Access Control Policy
- 24.7.1.3 Information Classification Standard
- 24.7.1.4 Security Incident Response Policy
- 24.7.1.5 IT Asset Disposal Standard
- 24.7.1.6 Cryptography Policy

24.7.2 Related Industry Best Practices, Policies & Standards

- 24.7.2.1 [OWASP Top 10 - Implement Security Logging and Monitoring](#)
- 24.7.2.2 [NIST SP 800-92 - Guide to Computer Security Log Management](#)
- 24.7.2.3 [NIST 800-171](#)
- 24.7.2.4 Sarbanes-Oxley Act (SOX) of 2002
 - 24.7.2.4.1 Although SOX applies primarily to financial and accounting practices, it also encompasses the information technology (IT) functions that support these practices.
 - 24.7.2.4.2 SOX can in part be supported by reviewing logs regularly to look for signs of security violations, including exploitation, as well as retaining logs and records of log reviews for future review by auditors.

24.8. Definitions & Terms

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

Certificate of Review

Information Logging and Monitoring Standard

March 24th 2026 12:10:08 pm

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Thursday, January 8, 2026 12:40 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, March 24, 2026 11:08 AM EDT
Mark Gutman		Policy Admin	Published	Tuesday, March 24, 2026 12:10 PM EDT