



Acceptable Use Policy

DOC-IT-IS-19
Revision 2.1
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	11/01/2024	Annual Review
2.1	11/01/2025	RXO, Inc updates, annual review

Table of Contents

1 Overview	4
1.1 Acceptable Use Policy Overview and Purpose	4
1.2 Scope	4
1.3 Policy Distribution	5
1.4 Relationship to Other Policies	5
1.5 Contacts	5
2 Policies	5
2.1 Credentials	5
2.1.1 Credentials Authorization	5
2.1.2 Review of Credentials	6
2.1.3 Change and/or Removal of Credentials	6
2.2 Use of RXOIS	6
2.2.1 User Responsibilities	6
2.2.2 Conditions of Use	7
2.2.3 Security and Integrity of RXOIS	8
2.2.4 Secure Computing Practices	8
2.3 Confidential, Sensitive, and Customer Information	10
2.4 Physical Security	10
2.5 Prohibited Activities	10
2.6 Monitoring	11
2.7 Profane Materials	12
2.8 Departure from RXO	12
2.9 Sanctions	13
2.10 Policy Review	13

1 Overview

1.1 Acceptable Use Policy Overview and Purpose

The RXO, Inc. (RXO) Acceptable Use Policy (the “Policy”) details the company-wide rules governing the secure operation and acceptable use of RXO Information Systems (RXOIS) and information assets. RXOIS is defined as all RXO owned, operated, or provided information technology-related hardware, software, equipment, facilities, and services.

RXO Global Security Office is committed to protecting RXO and its Subsidiaries and RXO’s employees from illegal or damaging actions by individuals, either knowingly or unknowingly. The publication of this Acceptable Use Policy is not intended to impose restrictions that are contrary to RXO established culture of trust and integrity. Because effective security is a team effort, it is the responsibility of every user, to know these guidelines and to conduct their activities accordingly.

Users are responsible for the safekeeping and security of RXOIS assigned to them or in their care. Users are expected to follow policies as developed and recommended by RXO to protect the security of RXOIS, including the physical security of RXOIS.

Use of RXOIS must be primarily for business-related purposes of RXO. Whilst we permit incidental use of our internet, email, and telephone systems to send personal email, browse the internet and make personal call telephone calls this is subject to the conditions set out in this policy, and any unauthorized use of RXOIS is strictly prohibited. Users should understand that they do not have a right or expectation of privacy in any information transmitted on RXOIS, except as provided for by applicable local laws. Personal use is a privilege and not a right and we may withdraw permission or restrict access at any time and at our discretion.

At all times, users must use due care when transmitting information of any kind using RXOIS.

Violations of this Policy will be reported to RXO management, and users who violate this Policy may be subject to discipline, termination, or legal action, as determined solely by RXO management according to the local law and collective labor agreements applicable to each country.

The relevant staff representative bodies have been duly informed and consulted regarding this Acceptable Use Policy.

Where relevant, agreements with unions were discussed and reached.

1.2 Scope

This Policy applies to users, defined as any and all users of RXOIS, individually or collectively, who are temporary, part-time, or regular full-time employees, agents, contractors, or third-party partners. This Policy applies to all RXO subsidiaries, divisions, and operating entities.

1.3 Policy Distribution

All users requiring credentials to access RXOIS will be informed of this Acceptable Use Policy and any revisions to it either by posting this Policy or revisions thereto in connection with users' access to RXOIS or otherwise distributing this Policy or revisions thereto to all users. RXO reserves the right to amend or revise this Acceptable Use Policy or supplement it with appendices for specific customer requirements and the like at any time at its sole discretion and without prior notice, subject to the appropriate information and consultation of the staff representative bodies where required by applicable law.

1.4 Relationship to Other Policies

This Policy supplements and does not supersede in its entirety or as a whole, any other RXO policies, including but not limited to any employment policies, harassment policies, e-mail policies, or document retention policies that may be in place. In the event that any particular provision of an RXO policy conflicts with this Acceptable Use Policy, then this Acceptable Use Policy is to be used in respect to RXOIS.

1.5 Contacts

Questions regarding this Policy should be directed to the Business Information Security Representative/Officer.

The representatives and/or Global Security Office team can be reached at security@RXO.com.

2 Policies

2.1 Credentials

2.1.1 Credentials Authorization

- 1) Credentials for RXOIS are requested by RXO management or a user and provided with appropriate manager approval.
- 2) Each Credential request and its approval(s) will be handled through a defined process and recorded.
- 3) As appropriate, Data Owners will approve Credential requests.

- 4) Each required approval must be completed for each request.

2.1.2 Review of Credentials

- 1) User credentials will be subject to periodic review by Data Owners and may be changed or terminated subject to section 2.1.3 below.

2.1.3 Change and/or Removal of Credentials

- 1) Whenever a user no longer needs credentials to RXOIS, or requires a change to credentials to RXOIS, the user's manager is responsible for notifying the Help Desk / HR immediately.
- 2) RXO will terminate a user's credentials immediately upon cessation of a user's employment with RXO, whether by way of termination or resignation.
- 3) RXO may change or terminate a user's credentials immediately and without notice where that the user no longer has an RXO company-related need to access RXOIS.
- 4) RXO may terminate a user's credentials immediately and without notice where that user has violated this Acceptable Use Policy in any way.
- 5) RXO may terminate a user's credentials immediately and without notice upon the suspension, of the user's employment with RXO.

2.2 Use of RXOIS

2.2.1 User Responsibilities

- 1) Users must comply with this Acceptable Use Policy, including the responsibility for compliance of same by any subordinate.
- 2) Use of RXOIS must be primarily for business related purposes of RXO.
- 3) Users must ensure that personal use of RXOIS is reasonable and does not affect RXOIS or result in unauthorized costs on the part of RXO or interfere with the user's or RXO's productivity. Personal emails must be labelled "Personal" or "Private" in the subject header. Personal use is a privilege and not a right and we may withdraw permission or restrict access at any time and at our discretion.
- 4) Users must abide by any other policies instituted by RXO regarding business and personal use of RXOIS.
- 5) Users must always use standard, RXO-approved e-mail signatures, without modification, on all transmissions or communications sent from a user's e-mail address and must not use non-business signatures or taglines (including, but not limited to personal quotes, jokes, icons, logos, or the like) in connection with e-mail messages.

- 6) Information resources may be used, provided unauthorized costs are not incurred, security, and system performance is not negatively affected, and copyright restrictions are not violated. Information resources include items such as, but not limited to, the following:
- 7) Online media, including but not limited to movies, videos, transmissions or postings on YouTube, webcam transmissions, music, or other media of any type, from any source including Skype.
- 8) Software, programs, or other intellectual property
- 9) Applications or services that incur costs for RXO including but not limited to ring tones, ring backs, games, premium text messaging services, alerts, donations, or other media or services for RXO - issued mobile and cellular telephones or portable mobile devices.
- 10) Electronic mail
- 11) Users must not install any unauthorized software on RXOIS.
- 12) Users must not transmit or send mass e-mails or other communications to publicize non-business issues, information, or events.
- 13) RXOIS systems must not be used for storage or transmission of hate, harassment, pornographic, or violent content.
- 14) Users must not create, forward, send, or transmit non-business-related messages, including "junk mail", "chain letters", "spam", or advertising material to individuals who did not specifically request such material.
- 15) Users must only use applications approved for use by RXOIS. If other applications are required, approval from local administrators must be obtained prior to use.

2.2.2 Conditions of Use

- 1) Users should understand that they do not have a right or expectation of privacy in any information transmitted on RXOIS, or content created, stored, transmitted, sent, or received on RXOIS, including but not limited to text messages, pages, e-mail, or any other transmissions or communications, except as provided for by applicable local laws.
- 2) Users are prohibited from using information technology-related hardware, software, equipment, or services that are not provided by or authorized by RXO for the performance of company-related work. Any exceptions must be formally approved by the CIO, CISO or their delegate.
- 3) RXO has the right to:
- 4) Deny or restrict a users' access to electronic information provided via RXOIS, including but not limited to web sites, web-based messaging, streaming media, social media, and e-mail.
- 5) Determine what Profane Material is.
- 6) Audit, inspect, and monitor RXOIS and users' use of RXOIS as set out in paragraph 2.8 below and subject to applicable local laws.
- 7) Prior to being granted access to RXOIS users must agree to comply with RXO information security policies and requirements.

- 8) RXO may remove credentials due to lack of use.

2.2.3 Security and Integrity of RXOIS

- 1) Users must access RXOIS only as directed by RXO.
- 2) Users must not allow unauthorized users to access RXOIS.
- 3) Users must not extend RXO' network by connecting to another network unless explicitly authorized by the Global Security Office.
- 4) Users must not connect unauthorized devices to the RXO network.
- 5) Users must report issues and incidents affecting the safekeeping or security of RXOIS to the Help Desk or to the Global Security Office, whether they are proven, presumed or suspected. Incidents that should be reported include, without limitation, the loss or disclosure of confidential information of RXO or of personal data of RXO employees, workers, or customers; security leaks or attacks; unlawful use of RXOIS; theft of RXO information or RXO property (intellectual property of RXOIS hardware)
- 6) Users are responsible for all activity performed under their credentials.
- 7) Users must not use another person's named account to login to RXOIS.
- 8) Users are responsible for the security of their credentials, taking necessary steps to prevent unauthorized access.
- 9) Users must keep credentials secure and private and must not share credentials. The Global Security Office and their designees will never ask users to share their credentials.
- 10) Users are required to ensure that all sensitive and confidential information in hardcopy or electronic form is always secure in their work area.

2.2.4 Secure Computing Practices

- 1) Users are responsible for the safekeeping and security of RXOIS devices or platforms assigned to them or in their care. For example:
 - a) PCs, laptops, workstations, and mobile devices must not be left unattended or unsecured. Laptops and mobile devices must be kept in the presence of the user and either taken with the user at the end of a working day or locked away securely.
 - b) Portable RXOIS devices must be protected to reduce the likelihood of loss or theft. Loss or theft must be immediately reported to the local Help Desk or Service Desk.
 - c) For mobile devices, screen lock, where available, must be enabled with a password.
- 2) Users must not interfere with the installation or operation of RXOIS features and capabilities provided for the secure and efficient operation of RXOIS (e.g., antivirus or backup capabilities).
- 3) Users must not attempt to validate suspected vulnerabilities on RXOIS. Any suspected vulnerabilities must be reported to the GSO.
- 4) To avoid security threats, users must use caution when using RXOIS. Appropriate behavior includes, but is not limited to:
 - a) Do not open e-mail attachments from unexpected sources.

- b) Do not open executable e-mail attachments (e.g., with the extensions “EXE”, “COM”, or “BAT”) from untrusted sources.
- c) Do not provide e-mail credentials or personal information requested by e-mail.
- d) Be alert for phishing attacks. Phishing is an attempt to trick users into taking an action, such as clicking on a link, opening an attachment, or completing a form. Although these actions seem harmless, attackers can gain instant access to user credentials or download viruses to user’s computer or perform other malicious actions. Best practices when it comes to phishing emails include, but are not limited to:
 - i. Be sure that the sender’s email address matches who they say they are (check the full name, @company name, etc.).
 - ii. Be extra cautious with emails coming from non-RXO senders. They are identified with a warning header: “[**Caution: External Sender, beware of Phishing**]”.
 - iii. Never initiate a transfer of money via email, even if the sender appears to be an RXO executive.
 - iv. Never click on links or respond to email to verify account or credential details, even if the email says to act quickly to avoid being locked out from your account.
 - v. Report suspicious emails by clicking on “Report Phishing” button on Outlook ribbon.
 - vi. Inform Information Security office immediately at InformationSecurity@RXO.com if you feel you have fallen victim to a phishing email.
- e) Be alert for social engineering attacks intended to tempt users into inadvertently defeating security measures. Social engineering attacks include, but are not limited to:
 - i. An e-mail addressed to an Internal User by name, including identifying information.
 - ii. A flash drive left to plant malware.
 - iii. A survey offering something in return for a password.
 - iv. An interesting e-mail message with a link to a malicious website.

RXO Global Security Office sends regular educational materials via emails and other means to educate our users on important security topics including phishing. Users are expected to read and understand this material and they should reach out with any questions. All users must also complete mandatory Information Security training within the time specified in each roll out.

Failure to complete information Security training, falling for phishing scams or other forms of social engineering attacks can lead to disciplinary action up to and including termination.

- 5) Users must pay special attention to system access in group environments, including but not limited to conferencing (e.g., teleconferencing, video conferencing, web meetings) and conference rooms. The meeting organizer is responsible for the monitoring system use and verifying logoff when the group session is complete.
- 6) Users may not use RXOIS to perform any security or port scanning without the approval of the GSO.
- 7) Executing any form of network monitoring which will intercept information not intended for the user is prohibited unless this activity is part of the user’s assigned duties.

2.3 Confidential, Sensitive, and Customer Information

- 1) Users are responsible for maintaining appropriate protection for Confidential, Sensitive, and Customer Information and must maintain protection while transferring such information. Copying Confidential, Sensitive, or Customer Information from a secure source to an unsecured location (including personal devices or personal email accounts) is prohibited.
- 2) Removable media used for storing Confidential, Sensitive, or Customer Information must be handled with the following measures:
 - a) Maintain security at all times by personal possession or locked storage.
 - b) Delete the Confidential, Sensitive, or Customer Information when it is no longer needed.
 - c) Encryption must be used.
- 3) If a user is unclear if information is Confidential, Sensitive, or Customer Information, they must contact the Data Owner to ascertain the information's classification.
- 4) Users are strictly prohibited from disclosing Confidential, Sensitive, or Customer Information without proper authorization from RXO Senior Management or accessing Confidential Information without authority or for purposes other than as required for work performed for RXO.
- 5) All printed media containing Confidential, Sensitive, or Customer Information must be disposed of by cross-cut shredding or through a secure disposal service provided by RXO.
- 6) Additional requirements for Customer Information may be specified in separate policies or documents.

2.4 Physical Security

- 1) Users must follow approved physical security procedures.
- 2) Users must prominently display a standard identification badge, if available, while in a data center, server room, or other RXO facility.
- 3) Proximity access cards, keys, and other physical access control devices are credentials and must be protected as such.

2.5 Prohibited Activities

The following activities are strictly prohibited:

- 1) Engaging in any activity that is illegal under local, state, federal, or international law while utilizing RXOIS.
- 2) Violating the intellectual property rights of any person or company, including, but not limited to, the installation or distribution of pirated or copyrighted software products that are not appropriately licensed for use by RXO.

- 3) Copying, without permission, other than appropriate fair use, of any copyrighted material, including but not limited to content from magazines, books, music, or other sources.
- 4) Recording Confidential, Sensitive, or Customer Information with devices, including, but not limited to, voice recorders or cameras, unless authorized by RXO Senior Management or the Global Security Office.
- 5) Any activity that significantly impacts the functioning or performance of RXOIS, significantly impacts the performance of business-related activities or responsibilities, results in unauthorized costs on the part of RXO, or otherwise causes or contributes to an appreciable impact on RXOIS, all as to be determined by RXO, Senior Management or the Global Security Office.
- 6) Accessing any websites or other Internet locations for purposes of gambling or engaging in any illegal activity.
- 7) Using RXOIS to access, upload, download, transmit, communicate, procure, or view Profane Material
- 8) Introducing Malware through negligence into RXOIS.
- 9) Revealing credentials to others or allowing unsupervised use of credentials or any other access to RXOIS by others, including other users.
- 10) Masking the identity of the user when using RXOIS.
- 11) Making fraudulent offers of products, items, or services originating from any RXO account
- 12) Engaging in phishing, scamming, or participating in any e-mail fraud of any type.
- 13) Effecting security breaches or disruptions of network communication.
- 14) Circumventing user authentication or security of RXOIS.
- 15) Using RXOIS for any purpose that is competitive to RXO or contrary to RXO' best interests.
- 16) Using RXOIS for the solicitation of non-company business or any use of RXOIS for personal gain.
- 17) Using RXOIS for the purpose of personal job-hunting or operating a personal income-generating business or activity.
- 18) Disclosing Confidential, Sensitive, or Customer Information outside RXO without proper authorization of RXO Senior Management.
- 19) Disruption of non-RXO systems, including, but not limited to, unauthorized access, hacking, denial of service, or disclosure of credentials.
- 20) The use of credentials other than your own.

2.6 Monitoring

- 1) RXO reserves the right to monitor and review any and all use of RXOIS to ensure compliance with this Policy. Our systems enable us to monitor telephone, email, voicemail, internet, and

other communications. Monitoring is only carried out to the extent permitted or as required by law and in respect of principles of relevance, proportionality, not excessiveness, and accuracy.

- 2) Monitoring of activities can be done through the activities of a user (username, email, windows login) or a device (IP, hostname). Purpose of monitoring is to protect RXO Network and systems, prevent security incident and detect threats.
 - a) Types of systems and usage include web filtering, antispam, machine health check, incident response, system logs.
 - b) What we monitor: All web activity except for healthcare and finance (banking) and all emails that transit via corporate email account, device activity, and system logs.
 - c) When we monitor: continuous monitoring of systems for Information Security purpose and upon specific request for Forensics purpose.
 - d) Data retention: Data is stored securely and is kept only if required by the purpose of the processing and in accordance with our Data Retention Policy and applicable local laws.
 - e) Access is limited and restricted to appropriate Information Security personnel.
- 3) To the extent permitted by local laws we reserve the right to retrieve the contents of email messages or files stored on workstations, or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business and for the following purposes:
 - a) To monitor whether use of the email system or the internet is legitimate and in accordance with this policy.
 - b) To find lost messages or retrieve messages lost due to computer failure.
 - c) To assist in the investigation of alleged wrongdoing.
 - d) To comply with any legal obligation.
- 4) **Reporting Violations:** Violations of this Policy will be reported to RXO management. Users who violate this Policy may be subject to disciplinary action, including termination or legal action, as determined by RXO management in accordance with local laws and collective labor agreements.

2.7 Profane Materials

No Profane Materials shall be transmitted through RXOIS. The creation, retrieval, access, or downloading of material that is offensive, sexually explicit, profane, or pornographic, is prohibited and will not be tolerated. RXO management has the sole right to determine whether language or imagery is abusive, profane, or potentially offensive.

2.8 Departure from RXO

Upon their departure from RXO, users must return all RXOIS equipment provided to them during the course of their employment in good general working order. They must not keep any equipment or data allowing access to RXO data or systems. Users must not destroy any RXO company information or data prior to their departure.

2.9 Sanctions

Any failure to comply with the rules and security measures described in this policy may result in limitations or suspensions of the right to use all or parts of the RXOIS, as well as disciplinary sanctions in accordance with the procedures provided for in RXO' internal regulations and in accordance with applicable laws. The acknowledged personal use of certain paid services through RXOIS may also give rise to reimbursement being required by the user.

RXO reserves the right to initiate or instruct the initiation of criminal proceedings regardless of the disciplinary sanctions implemented, in particular in the event of computer fraud, copyright infringement or violations in accordance with and as permitted by applicable local laws.

2.10 Policy Review

This Policy will be reviewed annually and updated as necessary to reflect changes in legal, regulatory, or business requirements.

Certificate of Review

Acceptable Use Policy

December 18th 2025 10:32:35 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Monday, November 24, 2025 11:39 AM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:00 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:32 AM EST