



Access Control Policy

DOC-IT-IS-O9
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

9.0 Access Control Policy	4
9.0.1 Executive Summary	4
9.0.2 Purpose	4
9.0.3 Scope	4
9.1 Business Requirements of Access Control	4
9.1.1 Access Control Policy	4
9.1.2 Access to Networks and Network Services	5
9.2 User Access Management	5
9.2.1 User Access Provisioning Deprovisioning	5
9.2.2 User Access Provisioning	5
9.2.3 Management of Privileged Access Rights	6
9.2.4 Management of Secret Authentication Information of Users	7
9.2.5 Review of User Access Rights	7
9.2.6 Removal or Modification of Access Rights	7
9.3 User Responsibility	8
9.3.1 Use of Secret Authentication Information	8
9.4 System and Application Access Control	8
9.4.1 Information Access Restriction	8
9.4.2 Secure Log-on Procedures	8
9.4.3 Password Management System	9
9.4.4 Use of Privileged Utility Programs	9
9.4.5 Access Control to Program Source Code	10

9.0 Access Control Policy

9.0.1 Executive Summary

9.0.1.1 This policy highlights the technological and procedural areas that RXO will address to affect a comprehensive Access Control approach as a key preventative control in RXO's Information Security Strategy. The objective is to ensure that all users have authorized access rights in accordance with the requirements of their role.

9.0.1.2 This policy defines the access control requirements surrounding the management of access to information assets on RXO's enterprise network as well as those assets residing in RXO cloud-based solutions. The purpose of this policy is to define security protection requirements that will further define the standards for the technical solutions to be implemented in the RXO operational environments.

9.0.2 Purpose

9.0.2.1 The purpose of the RXO Access Control Policy is to provide information security requirements for managing access to RXO systems, applications, networks, and information assets, ensuring that access is granted appropriately and securely.

9.0.3 Scope

9.0.3.1 This policy applies to all RXO subsidiaries, divisions, and operating entities, all full-time and part-time employees, agents, contractors, and third-party partners accessing RXO's systems, applications, networks, and information assets.

9.0.3.2 This policy covers all phases of identity and access management, including account provisioning, de-provisioning, and the management of access rights throughout the user lifecycle.

9.0.3.3 The policy applies to all classes of information, including sensitive and protected data, ensuring appropriate access control measures are in place.

9.1 Business Requirements of Access Control

9.1.1 Access Control Policy

9.1.1.1 RXO must communicate, publish, and review at least annually its Access Control Policy to ensure relevant business and information security requirements are adequately managed.

9.1.1.1.A RXO is committed to establishing and maintaining access to data, applications, systems, networks and network services in a manner that ensures maximized confidentiality, integrity, availability, possession, authenticity, and utility for these resources. In order to ensure controls are implemented in a comprehensive and effective manner, information security controls defined in this policy must align with business requirements. To ensure proper alignment, access controls identified and implemented must take into account, at a minimum:

- Security requirements;

- Legal requirements;
- Relevant legislative or regulatory requirements; and
- Relevant contractual requirements

9.1.2 Access to Networks and Network Services

9.1.2.1 Users must only be provided access to networks and network services required to perform their assigned job duties.

9.1.2.1.A Implement access controls for the networks and network services to enforce role-based access provisioning and management. Define controls, procedures, access control mechanisms, user authentication and monitoring requirements.

9.2 User Access Management

9.2.1 User Access Provisioning Deprovisioning

9.2.1.1 A formal user access provisioning and de-provisioning process must be implemented to manage the assignment and removal of users' access rights.

9.2.1.1.A All user and system access modifications must be processed through a formal methodology to ensure all assigned access is appropriately requested, approved, provisioned, and maintained throughout the access management lifecycle. These processes must ensure that unique user accounts are assigned to authorized individuals, implemented when needed, immediately disabled when users are terminated, or removed for the users or the system accounts that no longer require access.

9.2.1.1.B The use of shared, group, and generic user accounts is not permitted. An exception may be granted by following the RXO GSO Exception process. The owners of these accounts must maintain positive control and create and maintain documented lists of those employees who are able to access these accounts.

9.2.2 User Access Provisioning

9.2.2.1 A formal user access provisioning process must be implemented to approve or deny access request to systems, applications, networks, and network services.

9.2.2.1.A New users must be assigned a unique user account and granted access only after appropriately requesting and receiving approval for the requested access. Requests must follow a standard process that ensures appropriate security oversight is enforced, and appropriate authorization is obtained prior to account creation. Additional or modified access permissions may be assigned as requested by the user's management and approved by the appropriate data, application, or system owner(s). User accounts that are inactive for more than 90 days will expire.

9.2.2.1.B It is the responsibility of the onboarding manager to initiate the change process when an employee or contractor's role changes. All existing access rights for the user must be removed in a timely manner, and new rights requested as appropriate to the new role. If the role change requires the continuance of the old access, for the purpose of training to fill the position being vacated, the old access must remain provisioned for the time necessary to complete that training.

9.2.2.1.C Departing or terminated users must have their access rights disabled and/or removed immediately upon voluntarily or involuntary termination of employment, unless business needs or system technicalities require that the identity remain available. In this case, all authentication credentials must be immediately changed to prevent access by the original owner. It is the responsibility of the terminated employee's manager to initiate this process.

9.2.2.1.D All access must be specifically allocated to accounts and users based on approved roles and the concept of Least Privilege and need-to-know. Users' access must be reviewed and recertified at least annually.

9.2.3 Management of Privileged Access Rights

9.2.3.1 The allocation and use of privileged access rights must be restricted and controlled.

9.2.3.1.A Privileged or elevated access rights must be subjected to greater levels of reviews, monitoring, and approvals due to the inherent risk posed by privileged user accounts. All privileged access rights must be specific to the data, applications, systems, networks, and network services. In no case shall these rights allow complete administrative ability to all RXO systems, applications, and system utilities. All requests for privileged access must be authorized by the user's direct manager as well as the Information Owner. All access requests must include a written description of the business need.

9.2.3.1.B Privileged access rights must be controlled and specifically allocated to accounts and users based on approved roles and the concept of Least Privilege and need-to-know.

9.2.3.1.C Privileged access rights must be assigned to a user account different from those used for regular business activities; regular business activities must not be performed using privileged user accounts.

9.2.3.1.D Records of privileged access rights must be maintained in a dedicated repository, and all privileged accounts must be appropriately secured.

9.2.3.1.E Requirements for the expiration of privileged access rights must be defined, and all privileged accounts must be regularly reviewed.

9.2.3.1.F Generic and shared accounts are prohibited unless approved by both a Chief Information Officer (CIO) and Business Information Security Officer (BISO). The approved shared accounts must never be permitted to grant elevated levels of access. The approved accounts must enforce regular access requirements for all other accounts.

9.2.3.1.G It is prohibited to grant local workstation administrative access unless requested and approved by a Business Information Security Officer (BISO) or assigned delegate and/or as established by a formally Global Security Office (GSO) approved process.

9.2.4 Management of Secret Authentication Information of Users

9.2.4.1 The allocation of secret authentication information must be controlled through a formal management process.

9.2.4.1.A All users must take steps to protect secret authentication information, ensuring that authentication credentials and the access they provide are restricted to only approved personnel. All users must demonstrate understanding and agreement to these requirements by signing a statement to keep personal secret authentication information confidential and to prohibit the use of shared secret authentication information within the members of the group.

9.2.4.1.B Passwords must be protected at the time of issuance or update. To support this requirement, all initial passwords provided to users must be temporary, unique, not guessable, and require change on first use. All authentication credentials (initial or updated) must be delivered in a secure manner only following positive identification of the user's identity. At no time will such credentials be transmitted or communicated in an insecure manner via third parties or unencrypted text. Users must acknowledge the receipt of all secret authentication information, based on RXO approved methods.

9.2.4.1.C Default vendor secret authentication information must be changed or removed immediately following installation of systems or software.

9.2.5 Review of User Access Rights

9.2.5.1 Asset owners must review users' access rights at regular intervals.

9.2.5.1.A For critical systems, sensitive data repositories, and privileged accounts all user and system access must be reviewed at least annually by the appropriate asset owners and user managers, or their identified alternates. Such reviews must also be performed after any significant changes, including promotions, demotions, role changes, or termination of employment.

9.2.6 Removal or Modification of Access Rights

9.2.6.1 The access rights of all employees and external party users to information, information systems and information processing facilities must be removed upon termination or changes of their employment, contract, or agreement, or adjusted upon change.

9.2.6.1.A When an employee or contractor departs or is terminated, their access rights associated with information processing facilities and services (including to third party applications) must be removed or suspended. In cases where RXO believes that the individual departing the company may demonstrate aggressive behavior or become a risk to the company, the termination of access must be proactively disabled, including removing access prior to termination notification. It is the responsibility of the asset owner and/or the Leaver's manager to initiate this process.

9.2.6.1.B Users requiring modification or additional access due to a change in role must have their previously assigned access (including to third party applications) removed in a timely manner and follow a similar process as individuals that request new privileges and receive approvals from the appropriate parties. It is the responsibility of the asset owner and/or the requestor's manager to initiate this process.

9.2.6.1.C If periodic access reviews indicate that excessive privileges exist, the access rights must be removed.

9.2.6.1.D an employee, contractor, or external party user has access to or knowledge of password credentials to remaining generic or group IDs, these must be changed upon termination or change of employment, contract, or agreement.

9.2.6.1.E Any documentation that identifies access rights of users must also reflect the removal or adjustment of access rights.

9.3 User Responsibility

9.3.1 Use of Secret Authentication Information

9.3.1.1 Users must be required to protect the use of secret authentication information.

9.3.1.1.A User and system account password information must be secured and protected. All users must keep secret authentication information confidential, ensuring that it is not divulged to any other parties, including people of authority. At no time must authentication data be recorded (e.g., on paper, software file, or handheld device) unless it can be stored securely and the method of storage has been approved by the RXO Global Security Office.

9.3.1.1.B If there is any indication of possible compromise or unintended disclosure of secret authentication information, the RXO Global Security Office must be notified, and all affected passwords must be changed immediately.

9.4 System and Application Access Control

9.4.1 Information Access Restriction

9.4.1.1 Access to information and application system functions must be restricted based on individual business application requirements and in accordance with this access control policy.

9.4.1.1.A Applications and systems must be configured in a way that supports role-based and granular access levels. These platforms must support the ability to control access to system functions and data from users and other applications, limit specific access rights based on function (e.g., read, write, delete, and execute) and provide specific access to and isolation of data and the applications that support it.

9.4.2 Secure Log-on Procedures

9.4.2.1 Access to systems and applications must be controlled by a secure log-on procedure.

9.4.2.1.A All applications and systems in use by RXO must utilize suitable secret authentication information methods to substantiate the claimed identity of a user. At a minimum, all authentication methods must rely upon a username and password combination. Where strong authentication and identity verification is required, authentication methods that are alternative to passwords, such as cryptographic means, smart cards, tokens, or biometric means, must be used.

9.4.2.1.B All computing platforms must display a general warning notice that identifies the private ownership of the application or system, including cautions against unauthorized use and potential legal repercussions.

9.4.2.1.C At no time must RXO computing platforms display system or application identifiers during the log-on process. This includes not providing help messages during the log-on procedure that would

aid an unauthorized user or displaying passwords as they are being entered. All passwords must be masked upon entry.

9.4.2.1.D Authentication mechanisms must be self-protecting against local or networked compromise attempts whenever possible. The platforms must validate the log-on information only on completion of all input data and generate security alerts if a potential attempted or successful breach of log-on controls is detected. When successful authentication occurs, welcome screens must display the date and time of the previous successful log-on and the details of any unsuccessful log-on attempts since the last successful authentication. If an error condition arises, details must not be provided as to which part of the entry was correct or incorrect.

9.4.2.1.E All RXO applications and systems must be configured to protect themselves against compromise efforts. Systems and applications must follow the RXO Password Management standard.

9.4.2.1.F Use of biometric protection mechanisms on mobile devices is acceptable, if they only unlock the device password authentication for a user, but do not unlock underlying application authentication.

9.4.3 Password Management System

9.4.3.1 Password management systems must be interactive and must ensure quality passwords.

9.4.3.1.A Password management systems must be developed, documented, and implemented to support established password requirements. These password management systems must enforce the use of individual user account and passwords to maintain accountability.

9.4.4 Use of Privileged Utility Programs

9.4.4.1 The use of utility programs that might be capable of overriding system and application controls must be restricted and tightly controlled.

9.4.4.1.A The use of utility programs that might be capable of overriding system and application controls must be limited by both the availability of such applications and by constraining the minimum practical number of trusted, authorized users who have access rights to such software. Such applications must be formally approved and periodically reviewed by Infosec or must be removed or disabled upon detection.

9.4.4.1.B Where the utility programs are authorized, they must be configured to the approved levels of authorization, segregated from other applications, and accessible to only those users authorized such access.

9.4.4.1.C Regardless of location, all access to and functions of utility programs must require successful user authentication and be logged and monitored.

9.4.4.1.D Logs of how privileged utility programs are being used must be maintained.

9.4.5 Access Control to Program Source Code

9.4.5.1 Access to program source code must be restricted.

9.4.5.1.A Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) must be strictly controlled to prevent the introduction of

unauthorized functionality, avoid unintentional changes, and maintain the confidentiality of valuable intellectual property.

9.4.5.1.B Program source code must be controlled in secure centralized designated storage areas, preferably in program source libraries and not on operational systems. The program source code and the program source libraries must be managed according to established procedures, including limiting access to authorized support personnel, strict adherence to change control procedures and carefully logged and monitored.

9.4.5.1.C Program source code intended for publication must have additional security control measures and approvals to ensure integrity.

Certificate of Review

Access Control Policy

December 18th 2025 11:03:56 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Tuesday, November 25, 2025 2:24 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:28 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 11:03 AM EST