



Password Management Standard

DOC-IT-IS-21-1-3
Revision 2.0
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	11/01/2022	Initial Version
2.0	11/01/2025	RXO, Inc updates, annual review

Table of Contents

Security Standard – Password Management.....	4
Executive Summary	4
Purpose.....	4
Scope	4
Password Requirements	4
Password Best Practices and Recommendations	5
Password Standards	6
Initial Passwords	6
Password Protection.....	6
Password Storage	7
Password Sharing.....	7
Password Resets	7

Security Standard – Password Management

Executive Summary

Passwords are a vital aspect of information security. Passwords are the most commonly used method of securing information. A poorly chosen password may result in unauthorized access and/or manipulation of RXO, Inc. including its subsidiaries, divisions, and any other operating entities (collectively, “RXO”) resources. This standard defines the minimum requirements for the secure use of passwords.

Stronger forms of authentication may be necessary depending upon the situation.

Purpose

The purpose of the RXO Password Management Standard is to provide information security requirements for the processes related to managing the secret authentication information of users and systems.

Scope

All accounts that utilize a password, passphrase, or PIN as an authentication secret are in scope for this standard. This standard will provide guidance for the creation of strong passwords, the protection of those passwords, and how often they must be changed.

All users, including agents, contractors, and vendors with access to RXO systems, are responsible for taking the appropriate steps to select and secure their passwords.

Systems or processes that cannot comply with these standards require an exception from the GSO.

Password Requirements

The following specifications apply to all passwords. Exceptions for specific types of accounts will be listed where necessary.

- Passwords, including temporary passwords, must not be easily guessed or obtainable. A password should not include information such as a telephone number, birthdate, or location code. For example
“Welcome1!” or “1Password#” must not be used.
 - A password must not be a single word found in a dictionary.
 - A password must not contain the user id or account name, either in whole or part.
 - A password must not contain 3 or more consecutive identical characters.
- The password complexity must include the following character types.
 - Lowercase letters.

- o Uppercase letters.
 - o Numbers.
 - o Special characters.
- Minimum Password Length:
 - o Named accounts* – 12 characters or longer.
 - o Generic accounts** – 12 characters or longer.
 - o PIN protected devices – 6 digits or longer.
- Maximum password duration:
 - o Named accounts* – 90 days.
 - o Generic accounts** – 12 months.
 - o All other accounts – 90 days.
- The previous 24 passwords may not be reused.
- After no more than five (5) failed attempts, the account must be locked for 30 minutes. After the lockout period passes the account should automatically be unlocked.

* Named accounts are defined as accounts assigned to an individual

**Generic accounts are defined as user, system, service accounts that are not assigned to an individual or are designed to be used by more than one person or process.

Password Best Practices and Recommendations

- Use a passphrase instead of a password. A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters.
 - o Example passphrases:
 - § IncorrectHamster##BatteryTape@993#@
 - § ThesearetheLyricstomyfavoritesong \$\$
- “Th3reign1nEspañastaysMITplain.”
- At least 1 upper case, numeric, or special character should be somewhere in the middle of the password.
- A single password should not be used for business and non-business purposes. Example, using your home email password as your work computer password.
- Do not use words commonly found in a dictionary. This includes words from a foreign language, slang, dialect, or jargon. This is acceptable if used as part of a longer passphrase, see examples above.

- Do not use information that is easy to locate, such as personal information (Name, birthdays, pets, etc.) or work-related information (building name, site code, business unit, etc.).
- Avoid using patterns of letters or numbers. Ex. AaBbCc, 123321, or QWERTY.
- Avoid commonly used substitutions – such as 0 for o and 1 for i.
- Avoid frequently used character locations.
 - Most passwords start with an Uppercase letter.
 - Most passwords end with either a number or symbol
 - § The most common number is 1
 - § The most common symbol is !
- When using a password management tool, enabling multifactor authentication is highly recommended.

Password Standards

Initial Passwords

- A user's identity must be verified prior to providing a new, replacement, or temporary password.
- When a password is set by anyone other than the end-user, a temporary one-time password should be sent to the end-user, or their manager for first time users, that must be changed upon first use.
- All temporary passwords must be transmitted through a secure method. The use of a third-party or unprotected methods (such as a plaintext email outside the RXO network) should be avoided.
- Default vendor passwords must be changed after initial installation.

Password Protection

- Passwords are classified as Sensitive information.
- Passwords should not be reused. Passwords should be different for different systems.
- Do not hint at the format of a password in password reminders or security questions (for example, "my family name").
- Information Security may perform random testing to check the strength of passwords that are in use.
- Any password that fails must be changed.

Password Storage

- Do not write down a password, either on paper or in an electronic file, unless this is stored in a secure, approved manner.
- Do not store passwords in unencrypted files.
- Do not use the “Remember Password” function of a web browser. These features are insecure and do not provide the required protection.
- If a password is kept in an electronic file, a password management tool must be used to secure the stored passwords.

Password Sharing

- Do not share named account passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, or family members.
- The password for a generic (shared) account must only be known by members of the group authorized to use the shared account.
- Shared passwords must be changed whenever someone who knows the password leaves the company.
- Passwords should not be inserted into email messages, Skype messages, or other forms of electronic communication. This includes questionnaires, forms, or help requests.
 - The new employee onboarding process is exempt from this requirement.
- If an account name and password is shared via email the account name or file should be shared via a different channel such as a separate email message, a text message, or phone call.

Password Resets

Change Password

- A Change of Password occurs when the user knows the current password.
- Changing the password involves only the owner of the account, and the process must require submitting the current password.
- The new password is valid for the normal password duration.

Forgotten Password

- A Forgotten Password happens when the user does not know the current password.
- Forgotten passwords require the assistance from an administrator or a system to reset the password to a known value.
- Only the user may request a password reset. A manager may only verify the user's identity.

- The administrator resetting the password must verify the user's identity. Valid methods for verifying a user's identity include:
 - Correctly answering at least one security questions on file for the user.
 - A unique PIN sent to the user via SMS to a phone number on record to repeat back to verify identity.
 - A manager can verify a user's identity if the manager's identity is verified first. In this case the reset password must be sent to the manager.
- The new password must be a one-time password. After initial use, the user must change the password.
- An automated forgotten password service may be used if alternate identity verification information has been pre-established for a user. Examples include a recovery email address or security questions.

A password reset email must be sent to the user when a password has been reset.

Certificate of Review

Password Management Standard

December 18th 2025 10:34:20 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Monday, November 24, 2025 11:15 AM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:03 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:34 AM EST