



Cryptography Policy

DOC-IT-IS-10
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

10.0 Cryptography Policy	4
10.0.1 Purpose	4
10.0.2 Scope	4
10.1 Management Direction for Information Security	4
10.1.1 Policies for Information Security	4
10.1.2 Key Management	5

10.0 Cryptography Policy

10.0.1 Purpose

10.0.1.1 The purpose of the RXO, Inc. (RXO) Cryptography Policy is to outline requirements for the use of encryption technology to protect the confidentiality, availability, integrity, authenticity, possession, and/or utility of RXO's information assets.

10.0.2 Scope

10.0.2.1 This policy applies to all RXO subsidiaries, divisions, and operating entities, all employees, agents, contractors, and third-party partners, as well as all data and systems used by or supporting the company.

10.0.2.2 This policy applies to all sensitive information and other classes of protected information.

10.0.2.3 This policy applies to the processing and protection of regulated data which may include data elements from U.S. HIPAA data, U.S. Personally Identifiable Information (PII) (that is defined by U.S. State breach notification laws), and other (RXO defined) sensitive data. It includes GDPR Personal Data (which includes the processing of personal data of European Union (EU) citizens by RXO within the EU, and the processing by a controller (RXO) or processor (potentially RXO or a third party) that are outside of the EU. If the party outside the EU is (1) offering goods or services to the EU citizen or (2) monitoring the behavior of the EU citizen in so far as that behavior takes place in the EU, GDPR regulations will be very likely to apply.

10.1 Management Direction for Information Security

10.1.1 Policies for Information Security

10.1.1.1 Cryptographic controls must be in place for the protection of information that must be implemented for the use of cryptographic controls across the company as addressed in this policy, including the general principles under which business information must receive protection. The required level of protection, based on a risk assessment, taking into account the type, strength, and quality of the encryption algorithm prerequisites must be considered.

10.1.1.1.A Key management practices must be addressed, including methods to deal with the protection of cryptographic keys, the recovery of encrypted information in the case of loss, compromise or damage of the keys; and roles and responsibilities, e.g., who is responsible for the implementation of the policy and the key management, including key generation.

10.1.1.1.B All applicable regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world, including situations that may result in trans-border flow of secure information, must be considered when defining appropriate and acceptable use of cryptography.

10.1.1.1.C Cryptographic controls must be in place to achieve information security objectives, including the use of encryption of information to protect the confidentiality of information that is classified.

10.1.1.1.D Procedures must be included to address the appropriate use of encryption for protection of information during transmission by mobile or removable media devices or across communication lines.

10.1.1.1.E RXO must protect designated sensitive and regulated data using AES-128 Encryption or stronger with an effective key length of 128 bits.

10.1.2 Key Management

10.1.2.1 This policy applies to the development, protection, and implementation of cryptographic keys.

10.1.2.1.A A key management standard for each applicable environment must be implemented to identify requirements for effectively managing cryptographic keys throughout their entire lifecycle including generating, storing, archiving, retrieving, distributing, recovering, retiring and destroying keys.

10.1.2.1.B The standard must require the use of cryptographic algorithms, key lengths and other practices that are in alignment with Industry Information Security Best Practices.

10.1.2.1.C The standard must include appropriate key management processes that utilize secure practices for generating, storing, archiving, retrieving, distributing, retiring and the destruction of cryptographic keys.

10.1.2.1.D RXO must fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of RXO defined sensitive data.

10.1.2.1.E All cryptographic keys must be protected against modification and loss, secret and private keys must be protected against unauthorized use as well as disclosure, and equipment used to generate, store and archive keys is physically protected from unauthorized access.

10.1.2.1.F Activation and deactivation dates for keys must be formally defined in order to reduce the likelihood of improper use.

10.1.2.1.G Authentication processes used to verify and manage secret/private keys must use public key certificates issued by a reputable certification authority (CA) with suitable controls and procedures in place to provide proper oversight and a high degree of trust.

10.1.2.1.H The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g., with a certification authority, must address issues of liability, reliability of services and response times for the provision of services.

10.1.2.1.I In the event of a cryptographic failure, such as key compromise or an algorithm vulnerability, RXO must have an incident response plan that includes steps to revoke affected keys, re-encrypt sensitive data, and notify relevant stakeholders where needed.

Certificate of Review

Cryptography Policy

December 18th 2025 10:16:49 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 3:09 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 10:57 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:16 AM EST