



Secure Cipher Standard

DOC-IT-IS-36
Revision 1.0
MARCH 13, 2026

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	03/13/2026	Initial Version

Table of Contents

35 Secure Cipher Standard	4
35.1 Executive Summary	4
35.2 Purpose	4
35.3 Scope	4
35.4 Secure Cipher Standard Statements.....	5
35.4.1 Governing Policy and Alignment	5
35.4.2 Cryptographic Control Baseline	5
35.4.3 Minimum vs. Preferred Cipher Matrix.....	5
35.4.4 Prohibited Ciphers and Configurations	6
35.4.5 Key Management Requirements.....	6
35.5 Roles & Responsibilities.....	7
35.5.1 Information Security / GRC	7
35.5.2 Application Teams.....	7
35.5.3 Database Teams.....	7
35.5.4 Platform Server Teams	7
35.5.5 Integration Teams	8
35.6 Compliance	8
35.7 Exceptions.....	8
35.8 Review & Updates.....	8
35.9 References	8
35.9.1 RXO References	8
35.9.2 External References.....	9
35.10 Definitions.....	9

35 Secure Cipher Standard

35.1 Executive Summary

This Secure Cipher Standard defines the approved cryptographic ciphers, protocols, and configurations required to protect RXO information assets. The standard operationalizes the RXO Cryptography Policy (DOC-IT-IS-10) by specifying which ciphers are permitted, which are prohibited, and how they must be implemented across RXO environments to ensure confidentiality, integrity, and authenticity of data.

35.2 Purpose

The purpose of this document is:

- ☐ Establish a consistent, secure baseline for cryptographic cipher usage at RXO.
- ☐ Reduce exposure to weak, deprecated, or vulnerable encryption algorithms.
- ☐ Support regulatory, customer, and audit requirements.
- ☐ Enable secure interoperability across applications and infrastructure.
- ☐ To protect sensitive customer data.

35.3 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 applies to all RXO-managed systems, applications, services, and infrastructure across all environments and all data classifications requiring encryption.

35.4 Secure Cipher Standard Statements

35.4.1 Governing Policy and Alignment

- 35.4.1.1 RXO Cryptography Policy (DOC-IT-IS-10)
- 35.4.1.2 RXO Information Security Policy (DOC-IT-IS-05)
- 35.4.1.3 RXO Secure Server Standard (DOC-IT-IS-29)
- 35.4.1.4 Where conflicts exist, the more restrictive requirement applies.

35.4.2 Cryptographic Control Baseline

- 35.4.2.1 New systems MUST meet the Preferred / Target State standards unless a formally approved exception is granted. Existing systems must meet Minimum Acceptable standards and maintain a remediation roadmap.

35.4.3 Minimum vs. Preferred Cipher Matrix

Cryptographic Use Case	Minimum Acceptable	Preferred / Target State
Data at Rest Encryption	AES-128	AES-256
Disk / Volume Encryption	AES-128 (FIPS validated)	AES-256 (FIPS 140-2/140-3)
Database Encryption	AES-128	AES-256 with centralized key management
Backup / Object Storage Encryption	AES-128	AES-256 with customer-managed keys
Transport Protocol	TLS 1.2	TLS 1.3
TLS Cipher Type	AEAD (AES-GCM)	AEAD (AES-GCM or ChaCha20-Poly1305)
Key Exchange	ECDHE	ECDHE with modern curves
Asymmetric Encryption	RSA 2048	RSA 3072 or ECC P-256/P-384
Digital Signatures	RSA 2048 / SHA-256	ECC P-256+ / SHA-384+
Hashing / Integrity	SHA-256	SHA-384 or SHA-512
Certificate Key Size	2048-bit RSA	ECC or 3072-bit RSA
Key Storage	Software-based key vault	HSM or cloud-native KMS

35.4.4 Prohibited Ciphers and Configurations

Category	Prohibited Cipher / Configuration	Reason	Notes
Symmetric Encryption	DES	Insecure key length	All implementations prohibited
Symmetric Encryption	3DES	Deprecated by NIST	Sweet32 vulnerability
Symmetric Encryption	RC2, RC4	Cryptographically broken	RC4 prohibited in TLS
Symmetric Encryption	Blowfish (new)	Weak block size	Legacy only with exception
Transport Protocol	SSL (all versions)	Obsolete	SSLv2, SSLv3
Transport Protocol	TLS 1.0 / 1.1	Deprecated	Must be disabled
Key Exchange	Static / non-ephemeral	No forward secrecy	RSA key exchange
Hashing	MD5	Collision attacks	Never permitted
Hashing	SHA-1	Cryptographically weak	Including signatures
Certificates	Self-signed certificates (prod)	Lack of trust	Exception required
Key Management	Hard-coded cryptographic keys	High risk	Source code/configs
Key Storage	Plaintext private keys	Compromise risk	Repos/filesystems

35.4.5 Key Management Requirements

- 35.4.5.1 Keys must be generated, stored, rotated, revoked, and destroyed in accordance with the RXO Cryptography Policy.
- 35.4.5.2 Key rotation intervals must align with system criticality and regulatory requirements.
- 35.4.5.3 Compromised or suspected compromised keys must be revoked immediately.
- 35.4.5.4 Key management responsibilities must be clearly assigned and documented.

35.5 Roles & Responsibilities

35.5.1 Information Security / GRC

- 35.5.1.1 Define and maintain this standard.
- 35.5.1.2 Approve cipher-related exceptions.
- 35.5.1.3 Monitor emerging cryptographic risks.

35.5.2 Application Teams

- 35.5.2.1 Implement approved cipher configurations.
- 35.5.2.2 Disable deprecated and weak algorithms.
- 35.5.2.3 Ensure systems are configured in accordance with this standard.
- 35.5.2.4 Remediate findings related to cipher weaknesses.
- 35.5.2.5 Validate application compatibility.
- 35.5.2.6 Engage Information Security for design or exception requests.

35.5.3 Database Teams

- 35.5.3.1 Implement approved cipher configurations.
- 35.5.3.2 Disable deprecated and weak algorithms.
- 35.5.3.3 Ensure systems are configured in accordance with this standard.
- 35.5.3.4 Remediate findings related to cipher weaknesses.
- 35.5.3.5 Validate application compatibility.
- 35.5.3.6 Engage Information Security for design or exception requests.

35.5.4 Platform Server Teams

- 35.5.4.1 Implement approved cipher configurations.
- 35.5.4.2 Disable deprecated and weak algorithms.
- 35.5.4.3 Ensure systems are configured in accordance with this standard.
- 35.5.4.4 Remediate findings related to cipher weaknesses.
- 35.5.4.5 Validate application compatibility.
- 35.5.4.6 Engage Information Security for design or exception requests.

35.5.5 Integration Teams

- 35.5.5.1 Implement approved cipher configurations.
- 35.5.5.2 Disable deprecated and weak algorithms.
- 35.5.5.3 Ensure systems are configured in accordance with this standard.
- 35.5.5.4 Remediate findings related to cipher weaknesses.
- 35.5.5.5 Validate application compatibility.
- 35.5.5.6 Engage Information Security for design or exception requests.

35.6 Compliance

Non-compliance with this policy may result in access restrictions to affected systems or disciplinary actions as per RXO's guidelines.

35.7 Exceptions

Any exceptions to this policy must be formally documented and approved in writing by the RXO Governance Risk and Compliance (GRC) team. Exceptions documentation must include a valid business justification and compensating controls. Exceptions are time-bound and subject to periodic review.

35.8 Review & Updates

This standard will be reviewed annually, in response to cryptographic vulnerabilities, upon major infrastructure or threat landscape changes, or as required due to changes in business, technical, or regulatory requirements.

35.9 References

35.9.1 RXO References

- 35.9.1.1 RXO Cryptography Policy
- 35.9.1.2 RXO Information Security Policy
- 35.9.1.3 RXO Secure Server Standard

35.9.2 External References

- 35.9.2.1 NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations
- 35.9.2.2 NIST SP 800-57 Recommendation for Key Management
- 35.9.2.3 ISO/IEC 27001 Information Security, Cybersecurity and Privacy Protection

35.10 Definitions

AES	Advanced Encryption Standard
TLS	Transport Layer Security
AEAD	Authenticated Encryption with Associated Data
GCM	Galois/Counter Mode
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
RSA	Rivest-Shamir-Adleman
ECC	Elliptic Curve Cryptography
SHA	Secure Hash Algorithms
HSM	Hardware Security Module
KMS	Key Management Services
DES	Data Encryption Standard
3DES	Triple DES
RC2	Rivest Cipher 2
RC4	Rivest Cipher 4
SSL	Secure Socket Layer
GRC	Governance, Risk, and Compliance
NIST SP	National Institute of Standards and Technology Special Publication
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission

Certificate of Review

Secure Cipher Standard

March 24th 2026 12:08:44 pm

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, March 13, 2026 12:52 PM EDT
Faisal Khan		Policy Approver	Approved	Tuesday, March 24, 2026 11:07 AM EDT
Mark Gutman		Policy Admin	Published	Tuesday, March 24, 2026 12:08 PM EDT