



Approved Messaging Services Standard

DOC-IT-IS-26

Revision 1.0

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	November 1, 2025	Initial version

Table of Contents

26.0 Approved Messaging Services Standard4

 26.0.1 Executive Summary4

 26.0.2 Purpose4

 26.0.3 Scope4

26.1 Standards Statement5

 26.1.1 Approved Messaging Platforms5

 26.1.2 Restricted Messaging Platforms (Use Requires Approval)5

 26.1.3 Prohibited Messaging Platforms5

26.2 Responsibilities6

 26.2.1 IT and Security Teams6

 26.2.2 System Administrators.....6

26.3 Compliance.....6

26.4 Exceptions6

26.5 Review and Updates6

26.0 Approved Messaging Services Standard

26.0.1 Executive Summary

This standard defines the approved messaging platforms for internal and external communication within RXO, with the goal of minimizing data leakage, unauthorized access, and regulatory non-compliance. Messaging applications are widely used for collaboration, but without proper controls, they can introduce significant security risks. By formalizing the use of secure platforms—primarily Microsoft Teams—and restricting others like WhatsApp Business to controlled scenarios, this standard supports the RXO's broader cybersecurity and compliance objectives.

This document aligns with RXO's Information Security Management System (ISMS) and complies with relevant frameworks such as ISO/IEC 27001, NIST SP 800-53, and applicable data protection laws

26.0.2 Purpose

The purpose of this standard is to:

- Define a list of approved messaging platforms for business communication.
- Establish controls for restricted messaging applications.
- Ensure secure handling of sensitive and confidential information.
- Support regulatory compliance and reduce exposure to cyber threats.

26.0.3 Scope

This standard applies to:

- This standard applies to RXO, Inc., including all subsidiaries, divisions, and operating entities. All directors, officers, employees, contractors, and third parties acting on behalf of RXO must comply with this policy.
- All employees, contractors, and third-party vendors communicating on behalf of RXO.
- All company-owned devices and systems, including mobile phones, desktops, laptops, and cloud services.
- All forms of business communication, including internal collaboration and external client engagement.

Excluded:

- Personal communication unrelated to company business.
- Messaging within explicitly approved sandbox or test environments.

26.1 Standards Statement

26.1.1 Approved Messaging Platforms

The following messaging platforms are approved for unrestricted business use:

Platform	Use Case	Security Features
Microsoft Teams	Internal collaboration, meetings	End-to-end encryption, MFA, audit logs
Outlook (Email)	Formal communication	Secure email protocols, DLP controls

All approved platforms must be accessed using company-managed accounts and devices with endpoint protection enabled.

26.1.2 Restricted Messaging Platforms (Use Requires Approval)

The following platforms may be used only with written approval from the RXO Information Security Team (InfoSec):

Platform	Use Case	Conditions for Use
WhatsApp Business	Client engagement in limited cases	Must be documented, monitored, and approved by InfoSec

Restricted platforms must:

- Be used only on company-managed devices.
- Have message backups disabled or encrypted.
- Be monitored for compliance with data handling policies.

26.1.3 Prohibited Messaging Platforms

The following platforms are not permitted for business communication under any circumstances:

- Facebook Messenger
- WeChat
- Personal WhatsApp accounts

Use of prohibited platforms may result in disciplinary action and must be reported to the Information Security Team immediately.

26.2 Responsibilities

26.2.1 IT and Security Teams

- Ensure the implementation of this standard across the company.
- Conduct regular audits to ensure compliance with this standard.

26.2.2 System Administrators

- Ensure only approved messaging apps are installed on company devices.
- Ensure required security features are enabled and enforced.

26.3 Compliance

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

26.4 Exceptions

Any exceptions to this policy must be approved in writing by the RXO Governance Risk and Compliance (GRC) team and must include a valid business justification.

26.5 Review and Updates

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

Certificate of Review

Approved Messaging Services Standard

December 18th 2025 10:41:21 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 2:22 PM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:25 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 10:41 AM EST