Security requirement

M365 Exchange Online

Deutsche Telekom Group

Version	1.2
Date	Dec 1, 2023
Status	Released

Publication Details

Published by
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Germany

File name	Document number	Document type
	8.07	Security requirement

Version	State	Status
1.2	Dec 1, 2023	Released

Contact	Validity	Released by
Telekom Security psa.telekom.de	Dec 1, 2023 - Nov 30, 2028	Stefan Pütz, Leiter SEC-T-TST

Summary
Microsoft Exchange Online is a hosted messaging solution that delivers email, calendars, contacts, and tasks from PCs, the web, and mobile devices. It is fully integrated with Azure Active Directory, allowing administrators to use Group Policy and other management tools to manage Exchange Online features throughout their environment.

Table of Contents

1. Introduction 4
2. Email Encryption 5
3. Malware & Spam Protection 6
4. Mail Transport 7
5. Logging & Detection 9

1. Introduction

This document was prepared on the basis of the requirements of the Group Security Policy. The present safety requirement serves, among other things, as a basis for approval in the PSA process. It also serves as an implementation recommendation for the requirements of the Group Security Policy in units that do not participate in the PSA procedure. These requirements must be taken into account during the planning and decision-making processes and apply to all M365 environments of the respective unit.

When implementing the security requirement, the priority national, international and supranational law must be observed. If compliance with the described requirements cannot be implemented or can only be implemented to a limited extent in individual cases, a risk assessment must be carried out together with a security and/or data protection expert (in accordance with the relevant requirement) and possible alternative protective measures must be coordinated.

2. Email Encryption

Req 1	In order to enable secure, encrypted email traffic via S/MIME, a secure and approved PKI infrastructure must be operated

In order to enable secure, encrypted email traffic via S/MIME, a secure and approved PKI infrastructure must be operated.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.07-1/1.2

3. Malware & Spam Protection

Req 2	The Common Attachment Types Filter must be used

To prevent malware from being distributed via attachments in emails, the Common Attachment Filter must be activated.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.07-2/1.2

Req 3	Exchange Online Spam Policies Must Be Used

In order to identify and block (acquired) accounts that send spam emails, the Exchange Online Spam Policies must be configured and activated.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 8.07-3/1.2

4. Mail Transport

Req 4	Emails may only be forwarded to allowed domains

In order to prevent data exfiltration via email, redirects outside the organization may only be carried out to permitted domains.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.07-4/1.2

Req 5	DKIM must be used for all Exchange Online domains

To prevent fake emails that look like they come from your own organization, DKIM must be used.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.07-5/1.2

Req 6	SPF must be used for all Exchange Online domains

To prevent fake emails that look like they come from your own organization, SPF must be used.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.07-6/1.2

Req 7	DMARC must be used for all Exchange Online domains

To prevent fake emails that look like they come from your own organization, DMARC must be used.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.07-7/1.2

5. Logging & Detection

Req 8	Mailbox auditing for all users must be enabled

To monitor the behavior of the users of a mailbox, mailbox auditing must be enabled for all users.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Denial of executed activities
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.07-8/1.2