Security requirement

M365 Dynamics

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
	8.05	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
M365 Dynamics is a suite of CRM and ERP applications that helps manage an organization and achieve better results through AI-powered insights

Table of Contents

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. Documentation

Req 1	Changes to security roles must be documented

Changes to the security roles specified by the platform operation must be explicitly documented at a suitable location in the SDSK.

Validity: Application 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

For this requirement the following warranty objectives are relevant:

ID: 8.05-1/1.2

Req 2	The respective environment of the application must be documented

The architecture or environment that uses M365 Dynamics must be explicitly documented at a suitable location in the SDSK.

Validity: Application 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
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 8.05-2/1.2

Req 3	The configuration of the MS Dynamic Apps ("Modules") used must be documented

The configuration of all MS Dynamics apps ("modules") used must be explicitly documented at a suitable location in the SDSK.

Validity: Application 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
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 8.05-3/1.2

Req 4	The connection of M365 Sharepoint Online must be documented

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

For this requirement the following warranty objectives are relevant:

ID: 8.05-4/1.2

Req 5	The connection of M365 teams must be documented

If a team integration is required in the specialist application, this must be explicitly documented at a suitable location in the SDSK.

Validity: Application 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

For this requirement the following warranty objectives are relevant:

ID: 8.05-5/1.2