Security requirement

M365 Sharepoint 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
	8.04	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

SharePoint is a site-based collaboration system that leverages workflow applications, list databases, and other Web Parts and security features to enable business teams to collaborate. SharePoint also allows the company using the platform to control access to information and automate workflow processes across business units.

The Microsoft cloud version of SharePoint, SharePoint Online, has numerous additional features for integration with other cloud applications and complements many Microsoft packages offered with an Office 365 or Microsoft 365 license.

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. Access Policies

Req 1	The security controls for restrictive access must be implemented at site-collection level

Since the implementation of the security controls at the site-collection level is more restrictive than the implementation at the tenant level, the security controls must be implemented at the site-collection level.

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

For this requirement the following warranty objectives are relevant:

ID: 8.04-1/1.2

Req 2	To access SPO from non-managed devices, a Conditional Access (CA) policy must be implemented

If SPO is accessed from non-managed devices, access must be made more restrictive. For this reason, a Conditional Access (CA) policy must be agreed and implemented to access SPO from non-managed devices.

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

For this requirement the following warranty objectives are relevant:

ID: 8.04-2/1.2

Req 3	Session timeouts must be implemented

To access SPO, the following session timeouts must be configured:

- Access from managed devices: 5 days
- Access from non-managed devices: 1 day

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: 8.04-3/1.2

3. Content Sharing

Req 4	If the option "Share with everyone" is selected for content sharing, then the user must explicitly confirm this

As soon as a user selects the option "Share with everyone" during content sharing, the system must explicitly inform them that they want to share content with everyone in the organization and what effects this could have. The user must then explicitly confirm his choice.

Validity: Platform operation

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

For this requirement the following warranty objectives are relevant:

ID: 8.04-4/1.2

Req 5	A disclaimer must be displayed the first time an externally shared content is accessed

If a user accesses an external shared content for the first time, a disclaimer must be displayed.

Validity: Platform operation

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

For this requirement the following warranty objectives are relevant:

ID: 8.04-5/1.2

Req 6	Content may only be shared externally with existing guest accounts

Content may only be shared externally with existing guest accounts. For this reason, the level must be set to "Existing Guests".

Validity: Platform operation

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

For this requirement the following warranty objectives are relevant:

ID: 8.04-6/1.2

Req 7	Guests must log in with the account to which the external content sharing invitation was sent

If an invitation is sent to a guest account with which content is to be shared externally, the account to which the invitation was sent must be used for the login.

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
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.04-7/1.2

Req 8	Guest accounts may only share content that they own

Users with a Guest account may only share content for which they are registered as the owner.

Validity: Platform operation

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

For this requirement the following warranty objectives are relevant:

ID: 8.04-8/1.2

4. Sharepoint Sites

Req 9	SPO Custom Scripts may not be used

SPO Custom Scripts may not be used. The following alternatives/workarounds can be used to achieve the same usability:

- Use of SFPx or Power Apps
- Teams need to get a Modern Team Site so that forms can be turned into Power Apps

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

For this requirement the following warranty objectives are relevant:

ID: 8.04-9/1.2