Security requirement

M365 General Requirements

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
	8.00	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 365 (M365) is Microsoft's cloud platform, which enables communication and digitization solutions in the digital workplace to be created and used through the interaction of various services. In addition to the online versions of Word or Excel various services for collaboration (MS Teams, Sharepoint Online), and your own productivity (Mail, Calendar, Notes), tools for the digital mapping of processes and the creation of applications based on M365 and Azure Services (Power Platform, MS Dynamics) are also available. The M365 Cloud is defined as an independent cloud, which is offered by Microsoft in addition to the Azure Cloud.

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. Tenant & IAM

Req 1	Modern Authentication must be enabled

To prevent weak authentication from being used to log in to at least the following services, Modern Authentication must be enabled in the M365 Tenant:

- Exchange Online
- Skype for Business
- Sharepoint Applications

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: 8.00-1/1.2

Req 2	Conditional Access (CA) must be used to prevent the use of legacy authentication

In order to prevent the use of weak authentication, so-called legacy authentication, a login that uses legacy authentication must be blocked by a suitable Condidtional Access Policy.

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: 8.00-2/1.2

Req 3	Multi Factor Authentication (MFA) must be enabled for each account using Conditional Access (CA)

To prevent the takeover of an account, e.g. through a password leak, every account that logs in to Azure Active Directory (AAD) via the Internet must use Multi Factor Authentication (MFA).

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: 8.00-3/1.2

Req 4	Password Protection for Active Directory must be enabled

To prevent the use of weak or leaked passwords, Password Protection for Active Directory 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

For this requirement the following warranty objectives are relevant:

ID: 8.00-4/1.2

Req 5	A password reset of a privileged or break-glass account must be alerted

In order to check whether the change of password of a privileged or a break-glass account was lawful, any change of password of these accounts must be alerted.

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: 8.00-5/1.2

Req 6	Access to the Azure portal must be regulated according to the need-to-know or least-privilege principle

Access to the Azure portal may only be performed by some employees in compliance with the principles of need-to-know and least-privilege.

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: 8.00-6/1.2

Req 7	Only Privileged Access Workstations (PAW) may be used for privileged access to the tenant

To prevent privileged account compromise, privileged access to the M365 Tenant may only be performed using Privileged Access Workstations (PAW). The PAW shall meet at least the following requirements:

- Use of a modern endpoint detection and response solution such as Microsoft Defender for Endpoint or comparable
- The PAW must not have direct contact with the Internet, access to the M365 environment must be carried out via a separate infrastructure for privileged access
- The PAW must be particularly hardened and encrypted
- Authentication at the PAW must be done using MFA
- The user must not have local administration permissions on the PAW

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: 8.00-7/1.2

Req 8	To document the privileged roles and authorizations used, an administration concept must be created

An administration concept must be created to document and trace the privileged roles and authorizations used within the M365 environment.

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: 8.00-8/1.2

Req 9	To protect identities, Microsoft Defender for Identity must be used

Microsoft Defender for Identity must be used to secure identities and detect abuse.

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: 8.00-9/1.2

Req 10	Defender for Cloud apps must leverage access controls and geo-blocking rules for privileged accounts

Microsoft Defender for Cloud Apps includes risk-based rules that detect unusual behavior or illogical actions. For example, if one authentication is made from one country and immediately afterwards a second one from an IP address of another country, it becomes visible within such a short period of time that this is logically not possible at all.

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: 8.00-10/1.2

Req 11	Cloud Service Provider (CSP) Administrative rights may not be used

Third parties (outside the platform operation) may not be granted CSP-delegated administration rights. Instead, a complete user account for the third party must be set up for such use cases, as this allows admin privileges to be assigned granularly.

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: 8.00-11/1.2

Req 12	Applications that use M365 services must be explicitly registered in the tenant

Applications that use M365 services must be explicitly registered in the tenant. Documentation, e.g. in the form of an interface agreement, must be prepared and signed.

Validity: Platform operation, 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

For this requirement the following warranty objectives are relevant:

ID: 8.00-12/1.2

3. Backend

Req 13	Every server that offers backend services for the M365 environment must be protected with a modern endpoint detection and response solution

Every server that offers backend services for the M365 environment must be protected with a modern endpoint detection and response solution, such as Microsoft Defender for Endpoint or similar

Validity: Platform operation, 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

For this requirement the following warranty objectives are relevant:

ID: 8.00-13/1.2

Req 14	A suitable centralized Mobile Device Management (MDM) solution must be used to access the M365 services

A suitable centralized Mobile Device Management (MDM) solution must be used to access the M365 services. A current OS level of the mobile device as well as a separation between private and business data as well as applications must be observed.

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: 8.00-14/1.2

4. Applications

Req 15	All applications that connect to M365 Services must use Web Account Manager (WAM)

All applications that connect to M365 Services must use Web Account Manager (WAM).

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: 8.00-15/1.2

Req 16	Only shared third-party apps, addons, bots, connectors, etc. may be installed and used by the user

For example, to prevent unnoticed data exfiltration from the tenant, only centrally released third-party apps, addons, bots, connectors, etc. be installed and used by the user.

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: 8.00-16/1.2

Req 17	The Admin-Consent Workflow must be activated

To prevent a normal user from granting access permissions from or to an application, the admin consent workflow must be configured and activated accordingly.

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: 8.00-17/1.2

5. Data Security

Req 18	Links for External Sharing with Anonymous Access must be timed

To make data exfiltration by an attacker more difficult, external sharing links that allow anonymous access must be limited in time.

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: 8.00-18/1.2

Req 19	Data Loss Prevention Policies (DLP) must be configured and implemented

To prevent data leakage, for example in the context of an attack by hackers or by inattention, Data Loss Prevention Policies (DLP) must be implemented at the client level in the context of the respective application as well as at the platform level where this is technically possible.

Validity: Platform operation, Application 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: 8.00-19/1.2

Req 20	Microsoft Information Protection (MIP) must be configured and implemented

To protect the data to be processed and stored in the M365, Microsoft Information Protection must be implemented at the client level in the context of the respective application as well as at the platform level, where this is technically possible according to the current state.

Validity: Platform operation, Application 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: 8.00-20/1.2

Req 21	Custer Lockbox must be used

The Customer Lockbox feature must be used to protect the organization's data to be processed and stored in the M365 vis-à-vis the provider and the traceability of access to the organization's data by employees of the provider.

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
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.00-21/1.2