Security requirement

# M365 Power Apps

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 |
|---|---|---|
| | 8.02 | Security requirement |

| Version | State | Status |
|---|---|---|
| 1.2 | Dec 1, 2023 | Released |

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

Summary
Power Apps is a suite of apps, services, and connectors, as well as a data platform that provides an environment for the rapid development environment where custom apps can be built for business needs. By leveraging Power Apps, you can quickly create custom business applications that connect to various online and OnPrem data sources, such as SharePoint Online, M365 Dataverse, MS Dynamics, SQL Server, etc.

# 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. Data Connectors

| Req 1 | Non-blockable data connectors must be approved by an approval process |
|---|---|

Before using the non-blockable Data Connectors, they must be described and released as part of a PSA procedure.

Validity: Platform operation

For this requirement the following threats are relevant:
- 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: 8.02-1/1.2

| Req 2 | External systems that are connected via Data Connector may only be used with authentication |
|---|---|

If external systems that are located outside your own organization are connected to a Power App using Data Connectors, authentication must be carried out on the external system.

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

For this requirement the following warranty objectives are relevant:

ID: 8.02-2/1.2

| Req 3 | Only released internal systems may be connected via Data Connector |
|---|---|

Internal systems of the organization must be released as part of a PSA procedure before being connected by a Data Connector.

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

For this requirement the following warranty objectives are relevant:

ID: 8.02-3/1.2

| Req 4 | Only approved authentication modes allowed to be used |
|---|---|

Only non-shared credentials or AAD connections may be used for each Data Connector.

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: 8.02-4/1.2

# 3. Logging & Detection

| Req 5 | Audit Logs & Anomaly Detection Must Be Enabled |
|---|---|

As part of the operation of the Power Apps, audit logs and anomaly detection must be activated and connected to the organization's SIEM.

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: 8.02-5/1.2

# 4. Power Apps

| Req 6 | Power apps must not be shared in the external community |
|---|---|

Created Power Apps may not be shared with other people or institutions outside the organization.

Validity: Platform operation, Application operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 8.02-6/1.2