Security requirement

M365 Power Automate

Deutsche Telekom Group

Version	2.2
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
	8.03	Security requirement

Version	State	Status
2.2	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
Power Automate is a service that can be used to create automated workflows between apps and services, e.B. to synchronize files, receive notifications and/or collect data.

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 Blockable Data Connectors must be approved by an approval process

Before using the 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

For this requirement the following warranty objectives are relevant:

ID: 8.03-1/2.2

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 via 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 or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 8.03-2/2.2

Req 3 Only approved internal systems may be connected via Data Connector

Internal systems of the organization must be approved 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
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.03-3/2.2

3. Logging & Detection

Req 4	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:
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 8.03-4/2.2

4. Access Policies

Req 5	To access the Common Data Service, a Conditional Access (CA) policy must be implemented

Only authorized persons or applications may access the Common Data Service. For this reason, a CA policy must be created and activated that only authorized roles and/or accounts allow access to the Common Data Service.

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: 8.03-5/2.2

5. Templates & Flows

Req 6	Templates may not be shared in the external community

Created templates 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: 8.03-6/2.2

Req 7	Flows must not be shared

Created flows must not be divided by the option "Share by adding users as co-owner to flow".

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: 8.03-7/2.2

Req 8	The option "Secure Inputs / Secure Outputs" must be activated when developing flows

During the runtime of a flow, logs containing both data and metadata are automatically generated. Any user who has access to the flow is able to extract it via XML export. The "Secure Inputs / Secure Outputs" option encrypts the data and metadata contained in the log. For this reason, created flows must have the option "Secure Inputs / Secure Outputs" enabled.

Validity: Platform operation, Application operation

Motivation: Reducing the probability of data exfiltration

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

For this requirement the following warranty objectives are relevant:

ID: 8.03-8/2.2