Security requirement

M365 Dataverse

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
	8.06	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
M365 Dataverse allows you to integrate data from different sources into a single store that can then be used in different services such as M365 Power Apps, M365 Power Automate, M365 Power BI or M365 Dynamics.

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	To access the Dataverse, a Conditional Access (CA) policy must be implemented

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

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: 8.06-1/2.2

3. Data Security

Req 2 Record-level security in Dataverse must be used

In order to be able to control and restrict access to the data, adequate record-level security must be implemented for each individual database.

Validity: 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: 8.06-2/2.2

Req 3 Field-level security in Dataverse must be used

In order to be able to control and restrict access to the data, adequate field-level security must be implemented for each individual database.

Validity: 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: 8.06-3/2.2

Req 4 The accessibility of the forms of a table must be limited

It must be ensured that the forms of a table in the Dataverse cannot be reached by everyone within the organization. For this reason, the corresponding option must be set to "Specify Security Roles" and the corresponding security roles must be implemented.

Validity: 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: 8.06-4/2.2

Req 5 Certain files in the form of attachments must be blocked

To minimize the likelihood of a ransomware attack or data exfiltration, for example, the following files must be blocked as attachments:
de,adp,app,asa,ashx,asmx,asp,bas,bat,cdx,cer,chm,class,cmd,com,config,cpl,crt,csh,dll,exe,fxp,hlp,hta,htr,htw,ida,idc,idq,inf,ins,isp,its,jar,js,jse,ksh,lnk, mad,maf,mag,mam,maq,mar,mas,mat,mau,mav,maw,mda,mdb,mde,mdt,mdw,mdz,msc,msh,msh1,msh1xml,msh2,m

sh2xml,mshxml,msi,msp,mst,
ops,pcd,pif,prf,prg,printer,pst,reg,rem,scf,scr,sct,sh,shb,shs,shtm,shtml,soap,stm,tmp,url,vb,vbe,vbs,vsmacros,vss,vst,
vsw,ws,wsc,wsf,wsh

Validity: Application operation

Motivation: Minimization of the attack surface

For this requirement the following threats are relevant:
- 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: 8.06-5/2.2

Req 6	To minimize the likelihood of attacks with the help of emails, the option "Use secure frames" must be activated

To minimize the likelihood of attacks with the help of emails, the option "Use secure frames" must be activated.

Validity: Platform operation, Application operation

Motivation: Minimization of attack surface

For this requirement the following threats are relevant:
- 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: 8.06-6/2.2

4. Logging & Detection

Req 7	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, 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

For this requirement the following warranty objectives are relevant:

ID: 8.06-7/2.2