E031- Microsoft 365 Application Directive

Directive on federal information technology

Classification:[1]	None
Binding force:[2]	Directive
Specification type:[3]	(E) Application directive
Planning area:[4]	Basic ICT services for the entire Federal Administration
This version:	2.0
Replaces version:	1.1
Status (this version):	Draft
Date of decree / Date of entry into force (this version):	Decree on ICT Steering: 21 February 2024 Entry into force: 21 February 2024
Enacted by, legal basis:	Delegate for Digital Transformation and ICT Steering (D-DTI), based on Article 17 paragraph 1 letter e of the Ordinance of 25 November 2020 on the Coordination of the Digital Transformation and ICT Steering in the Federal Administration (DTIO), SR 172.010.58
Languages:	German (original), French (translation), English (translation)

1 For the classifications INTERNAL and CONFIDENTIAL, see *Article 13 of the Information Security Act of 18 December 2020 (SR 128)*.

2 On the form of enactment and binding force, see *Federal Office of Justice: Legislative Guide, 4th edition 2019 (status: 2023)*.

3 See DTI-FCh information platform.

4 Planning areas as per the *Federal ICT Strategy 2020–2023 of 3 April 2020 (SB000)*.

Table of contents

1 General provisions

1.1 Object

[1] This directive governs use of the *Microsoft 365 platform* as part of the Standard Service Office Automation.

[2] Service providers (SPs) and service users (SUs) must comply with this directive in order to use Microsoft 365 services and other services based thereon.[5] Compliance with the directive ensures lawful use of the M365 platform and protection of Federal Administration data.

[3] The directive lays down rules for processing data on the *Microsoft 365 platform*. It supplements existing federal directives, departmental directives and other specifications issued by administrative units on the use of IT. Its implementation relies on the cooperation and personal responsibility of all Federal Administration employees.

1.2 Scope

[1] The scope of this directive is identical to that of *Article 2* of the *Ordinance on the Coordination of the Digital Transformation and ICT (DTIO).*

[2] The directive is binding for users of *M365* services forming part of the Standard Service Office Automation (SS OA).

[3] The binding force[6] of the individual provisions in section 2 of this directive is determined based on the keywords in Appendix D.

1.3 Definitions

[1] For the purposes of this directive, the following definitions apply:

a. *Microsoft 365 platform*: Microsoft 365 public cloud services provided by the Standard Service Office Automation. The platform is integrated into the Federal Administration's office automation environment and is therefore part of this environment.

b. *Microsoft 365 (M365):* Set of public cloud-based applications and functions for office automation, such as Teams, SharePoint Online, OneDrive for Business and administration and security tools, as well as *Microsoft 365 Apps for enterprise* installed locally on workstations.

c. The *M365 Portfolio* details the Microsoft 365 public cloud services approved by the Standard Service OA.

d. *M365 services*: Services used according to the *M365 Portfolio*.
These include the following:

1) Microsoft 365 Apps for enterprise (aka M365 Apps): Office applications installed locally on workstations (Teams, Outlook, Word, Excel, PowerPoint, OneNote, Access, etc.).

[5] For example, Contact Center, Attendant Console, shared line appearance, Teams apps, and many more.

[6] Binding force levels according to *Request for Comments: RFC 2119 (PCB 14), The Internet Engineering Task Force (IETF).* The specification of levels of binding force according to [RFC 2119] is a common practice in international standardisation.

2) *Microsoft 365*: Cloud-based office applications that can be used in a browser, such as Teams, Outlook Web Access, Word Online, Excel Online and PowerPoint Online.

3) *Exchange Online:* Exchange Online is used for email-related services. The service enables access to emails, calendars, contacts and tasks.

4) *Teams:* Cloud-based collaboration app. It features individual and group chat, video and audio conferencing, document and calendar sharing as well as the availability status of employees in a central workspace.

5) *SharePoint Online:* Cloud-based collaboration platform. SharePoint Online enables the Federal Administration to jointly store, use and manage content and applications.

6) *OneDrive for Business:* Personal cloud-based storage repository for personal and private data as defined in [E026]. Wherever possible, business data should be kept in the shared repositories or in the systems provided for this purpose.

7) *Viva Engage (formerly Yammer):* An enterprise social networking service. Geared to professional use, it focuses on the sharing and editing of documents, the exchange of knowledge, and internal and cross-company collaboration and communication. Within the Federal Administration, it is primarily used for communities of practice.

e. *Account Modern:* A user account according to the SS service catalogue, which is managed in on-premises Active Directory and replicated in Azure Active Directory. M365 services are only available with *Account Modern*.

f. *Workstation system (WSS) or workstation:* The workstation system consists of the ‘Workstation’ service [SS105] and the ‘Virtual Desktop’ service [SS119], which is offered in the SS OA in accordance with the SS service catalogue [SS100]. The workstation system is integrated into the Federal Administration’s office automation environments and enables access to its specialist applications.

[2] An overview of concepts and scope is presented graphically in Appendix B.

2 Microsoft 365 Application Directive

2.1 Responsibilities

[1] Together with the defined SPs, the SS OA provides standardised and centralised basic ICT services for workstations in accordance with the SS service catalogue [SS100].

[2] The SS OA ensures the provision of *M365 services* as well as basic IT protection [Si001].

[3] The departments and administrative units (service users) know the data and the business processes for which they wish to use M365. They are familiar with the requirements applying in their areas. They MUST therefore determine the data protection requirements on their own responsibility. They check whether the basic IT protection measures are sufficient for the data for which they are responsible. In particular, they must ensure that no unauthorised data as defined in section 2.2 paragraph 1 is processed on M365.

[4] Processed documents MUST be categorised, either by the users or by automated processes, according to their classification under the Information Security Act [ISA] and the Data Protection Act [FADP], and labelled accordingly.

[5] The departments and administrative units (service users) define further requirements and measures for their area of responsibility as required.

[6] The SS OA helps the departments and administrative units to assume the responsibilities set out in paragraph 3 (in particular by means of ICT tools, aids, training courses, etc.).

2.2 Data processing

[1] M365 MAY be used to process data up to the classification INTERNAL as defined in the ISA and ‘personal data’ as defined in the FADP.

The M365 services are expressly not authorised for data with a higher classification or for ‘sensitive personal data’ and ‘personality profiles’ under the FADP. Such data must be opened and processed using the locally installed Office version and the tools[7] approved for this purpose. It must be stored on the services approved for the administrative unit, e.g. GEVER or specialist applications.

Currently authorised usage of individual M365 services can be found in Appendix A.

[2] Unless prohibited by data processing regulations or a requirement of the administrative unit, information covered by official secrecy MAY be processed using M365 services.[8]

[3] The departments and/or administrative units SHOULD provide their employees with assistance in classifying information and categorising it in accordance with the FADP. As only the administrative units are familiar with their business and content, they MAY define organisation-specific rules for the use of M365.

---

[7] These currently include the SecureCenter encryption tools and the successor product CHCrypt.

[8] As set out in the legal basis analysis for Microsoft 365, the processing of data covered by official secrecy is permitted based on the agreements concluded with Microsoft and the amendment made to Article 320 of the Swiss Criminal Code (SCC) (see CEBA Project → Legal basis).

The document ‘Anforderungen angesichts des Risikos von Amtsgeheimnisverletzungen in der Bundesverwaltung’ (Requirements in view of the risk of breaches of official secrecy in the Federal Administration) [Si001-Hi03] sets out recommended actions to prevent breaches of official secrecy which may become relevant in connection with the disclosure of data to third parties in support cases. In case of doubt, it is advisable to consult the administrative unit’s legal service for an assessment.

[4] The *M365 services* SHOULD be used for business purposes in accordance with the Workstation System Application Directive [E026].

[5] Users MAY process business-relevant information temporarily using M365 services. Once the work has been completed, it MUST be entered back into the respective GEVER business management system or specialist application of the administrative unit.[9]

[6] Before any voice and/or video communication is recorded, the consent of all participants MUST be obtained.

[7] For every *Viva Engage* conversation, there MUST be at least one designated moderator who will intervene in the discussions if necessary (e.g. in case of verbal abuse, racism, discrimination).

2.3 General conditions of use

[1] Whenever this is offered by Microsoft, M365 services are operated within Switzerland and the data is kept on Swiss territory. Where this is not possible, the services are operated within the European Union (EU Data Boundary).[10]

[2] Certain M365 services are not available for reasons linked to public procurement law or security concerns. The range of available functions is described in the *M365 Portfolio*.

[3] To use *M365* services, the administrative unit (AU) orders the *'Account Modern'* market service from the SS service catalogue.

[4] Smart devices that are managed via the SP's Mobile Device Management (MDM) system MAY use M365 services without restriction.
All other private or third-party devices MAY only use the M365 services via online processing (Office Online) in the browser.[11]

[5] Approved means of authentication (e.g. smart card or other multi-factor authentication) MUST be used for full access to M365 services (login).[12]

[6] When registering on the *M365 platform* for the first time, users MUST confirm that they have taken note of and will comply with this application directive.

3 Final provisions

3.1 Compliance

[1] The departments and the Federal Chancellery shall ensure the implementation of this directive in their areas of responsibility in accordance with Article 3 DTIO.

[9] Ordinance on Electronic Records and Process Management in the Federal Administration (GEVER Ordinance, SR 172.010. 441) Article 4.

[10] Details of where Microsoft 365 stores customer data can be found at: https://learn.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide

[11] See also Appendix A Table 2. This is implemented by the service provider, including the relevant technology.

[12] This is implemented by the service provider, including the relevant technology.

3.2 Review

[1] The Digital Transformation and ICT Steering Sector of the Federal Chancellery (DTI Sector) shall review this directive no later than four years after it comes into force to ensure that it remains up to date and continues to fulfil its intended purpose.

3.3 Commencement

[1] The present version of this directive comes into force on 21 February 2024.

[2] For the CEBA Agil platform, version 1.1 will continue to apply until CEBA Agil is taken out of service.

Appendices

A. Use of *M365 services*

The following table shows permitted uses of core ***M365 services*** with regard to information and data protection.

Green: Permitted without restriction Yellow: Permitted with restrictions Red: Not permitted

Classification under FADP	**Classification under ISA**	**Local Office applications (installed on WSS)**	**M365 Online (Office web version)**	**Teams**	**SharePoint Online**	**OneDrive for Business**	**Viva Engage**	**All others** (e.g. Planner, To Do List)
Personal data	**INTERNAL**	Without restriction	Without restriction on managed end devices (WSS) Online processing only on non-managed end devices (e.g. private PCs)	Without restriction	Without restriction	Without restriction	Without restriction	Without restriction
Sensitive personal data and personality profiles	**CONFIDENTIAL**	Documents must be protected with an approved encryption system.[13] Processing only in the local SAFE area of the encryption environment. Storage in GEVER or a repository or application approved by the AU.	No processing permitted (no integration with the encryption tool[12])	No processing, storage or chat/audio/video communication permitted Other tools are available for this purpose.	No processing or storage permitted	No storage permitted	No processing or storage permitted	No processing or storage permitted
	SECRET	Not permitted	Not permitted	Not permitted	Not permitted	Not permitted	Not permitted	Not permitted

Table 1: Permitted uses of M365 services

[13] Approved encryption systems include SecureCenter and CHCrypt.

Permitted uses of M365 services on categories of end devices

The following table shows permitted uses from the perspective of different categories of end device.
M365 services may be used without restriction on end devices managed by the Federal Administration for personal data and data classified as ‘internal’.
M365 may be accessed from third-party devices either via the mobile VDI service (without restriction) or via a browser (only online tools can be used).
Access requires a Federal Administration account and an approved method of multi-factor authentication.
For data in higher categories, restrictions generally apply or use of M365 services is not permitted.

		End device		
Classification under FADP	**Classification under ISA**	**Fully managed WSS** (OA client) with locally installed Office application and OneDrive for Business (including mobile VDI)	**Partially managed** end device with federal MDM, such as smart device with locally installed Office mobile applications and OneDrive for Business	**Non-managed third-party device** (e.g. private PC, BYOD, private smartphone without MDM)
Personal data	**INTERNAL**	Usable without restriction	Usable without restriction	Only online processing on M365 via browser possible (M365 Office Online) (with Federal Administration account and multi-factor authentication) Exception: mobile VDI: usable without restriction
Sensitive personal data and personality profiles	**CONFIDENTIAL**	Documents must be protected with an approved encryption system. Processing only in the local SAFE area of the encryption environment. Storage in GEVER or a repository or application approved by the AU. Audio/video and chat communication are not permitted.	No processing, storage or chat/audio/video communication permitted (no integration with the encryption tool)	No processing, storage or chat/audio/video communication permitted (no integration with the encryption tool)

Table 2: Overview of the use of M365 services from the perspective of end devices

B. Overview of concepts

Application Directive E031 relates to use of the Microsoft 365 platform, which is shown separately in the figure. This is a schematic demarcation between the Microsoft 365 platform and the Federal Administration's existing office automation services. The diagram shows the relationships between the concepts used.

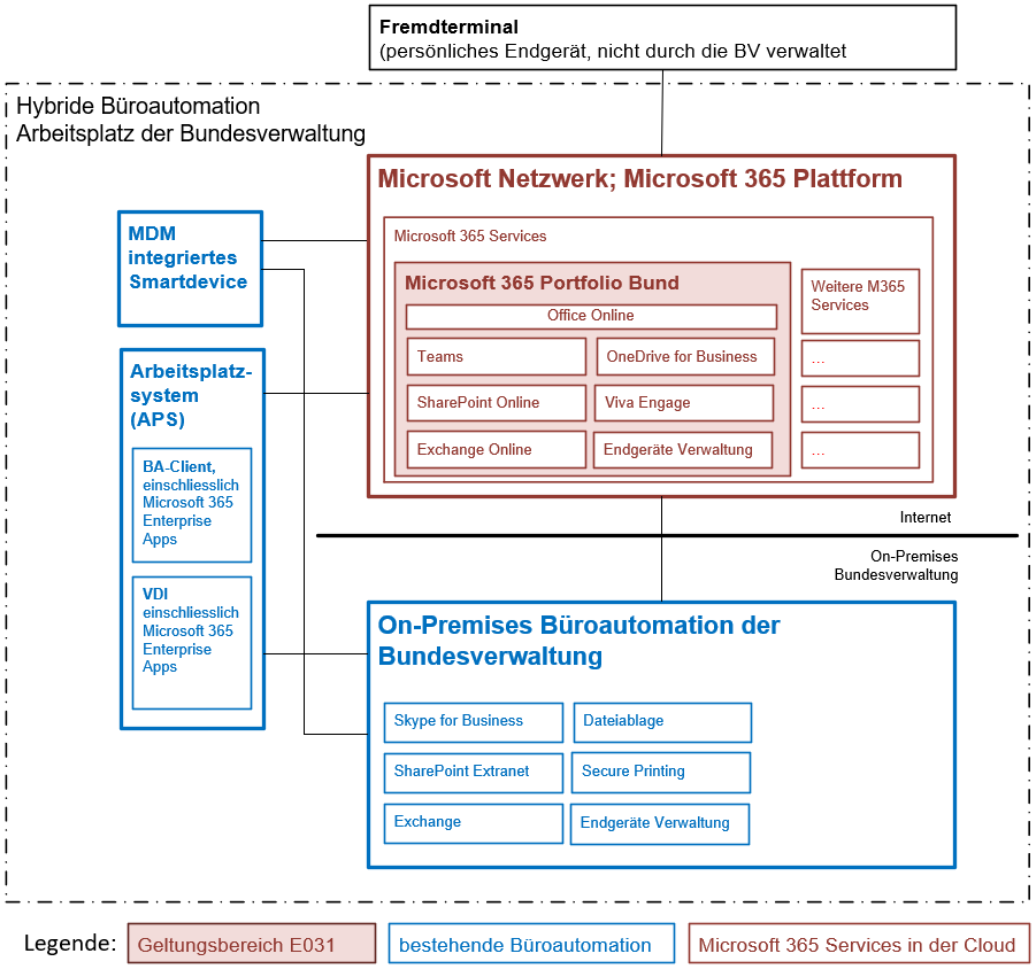

Figure 1: Overview of concepts

C. Changes from previous version

- Fundamental revision, with E031 V1.1[14] remaining applicable to CEBA Agil. The provisions have been adapted to the Microsoft 365 production environment.
- All FITSU-related wording has been adapted in accordance with the *Ordinance on the Coordination of the Digital Transformation and ICT* [DTIO].

D. Meaning of keywords relating to binding force level

The binding force[15] of the individual provisions in section 2 of this directive is indicated by the following keywords in capital letters:

Keyword	Binding force
MUST	Provision that must be complied with (except for granted exemptions)
MUST NOT	Option that is not allowed
MAY	Option is expressly permitted. The AU can decide whether or not to exercise the option. If the provision concerns an ICT solution, the provider of this solution must offer the option.
SHOULD	Option to be selected in normal cases. However, an AU may deviate from this without being granted an exemption by the FCh's DTI Sector or the NCSC provided this does not compromise cost-effectiveness and/or security. Any deviation from the provision must be justified in writing to the FCh's DTI Sector or the NCSC.
MAY	Accepted option. If the requirement concerns an ICT solution, the solution provider shall decide whether to support the option.

E. References

ID	Reference[16]
FADP	Federal Act of 19 June 1992 on Data Protection (Status as of 1 September 2023); SR 235.1
E026	E026 – Workstation System Application Directive
GEVER Ordinance	Ordinance on Electronic Records and Process Management in the Federal Administration; SR 172.010.441
ISA	Federal Act on Information Security in the Confederation (Information Security Act); AS 2022 232
InfoSecO	Ordinance on Information Security in the Federal Administration and Armed Forces (Information Security Ordinance); AS 2023 735
RFC 2119	Request for Comments: 2119 (PCB 14), The Internet Engineering Task Force (IETF)

[14] See https://intranet.dti.bk.admin.ch/isb_kp/de/home/ikt-vorgaben/einsatzrichtlinien/e031-ceba.html

[15] Binding force levels according to *Request for Comments: RFC 2119 (PCB 14), The Internet Engineering Task Force (IETF).* The specification of levels of binding force according to [RFC 2119] is a common practice in international standardisation.

[16] Enactments at federal level are referenced according to the Classified Compilation of Federal Legislation. In the case of a referenced federal requirement, the version valid on the date of decree of this directive is indicated.

ID	Reference[16]
SB000	SB000 - Federal ICT Strategy 2020–2023
SS100 - SS service catalogue	The ICT standard services (SS) service catalogue lists the services, service variants and options provided within the standard services. It is aimed primarily at the departmental integration managers (IMDs) and the service providers of standard services (SP-SS). SD100 - SS service catalogue
Si001	Si001 - IT baseline protection in the Federal Administration
Si001-Hi3	Si001 - Hi03: Anforderungen angesichts des Risikos von Amtsgeheimnisverletzungen in der Bundesverwaltung – Version 1.4
SCC Art. 320 (Official secrecy)	Official secrecy exists where there is a statutory duty of confidentiality and the facts in question are neither publicly known nor generally accessible and must not be disclosed in either the public or private interest (see Art. 320 para. 1 SCC).
DTIO	Ordinance on the Coordination of the Digital Transformation and ICT Steering in the Federal Administration (Ordinance on the Coordination of the Digital Transformation and ICT); SR 172.010.58

F. Abbreviations

Initials	Meaning
OA	Office automation
FCh	Federal Chancellery of the Swiss Confederation
CEBA	Cloud Enabling Office Automation programme
FADP	Data Protection Act
DTI	Digital Transformation and ICT Steering Sector of the Federal Chancellery
GEVER	Electronic business management system
ISA	Information Security Act
InfoSecO	Information Security Ordinance
ICT	Information and communication technology
MDM	Mobile Device Management
NCSC	National Cyber Security Centre
SS OA	Standard Service Office Automation
RFC	Request for Comments
AU	Administrative unit