Terms of Service for Guest Users for Collaboration in the FEV MS Collaboration Environment

Table of Contents

1. Objective of Terms of use

(1) The companies of the FEV Group, and in particular the FEV Company with which you or your organization have a business relationship (FEV), shall take appropriate technical and organizational measures (TOM) to ensure adequate security of confidential information and personal data within the scope of the autonomous determination of purposes and means of data processing as a data controller under the General Data Protection Regulation (GDPR). In addition to numerous TOMs, that are centrally specified and implemented by the FEV Group, compliance with technical and organizational data protection is also required by individual FEV employees as well as by external guest users.

(2) In order to protect the FEV MS Collaboration Environment, its users and data subjects affected by the data processing as well as in general to comply with applicable laws, this Terms of use addresses rules of conduct to be observed by guest users. They apply to all guest users collaborating via the FEV MS Collaboration Environment. By using the guest access, you as a guest user agrees to comply with the guidelines regulated herein. Existing regulations between FEV and the guest users and/or their organization, such as non-disclosure agreements ("NDAs"), remain unaffected.

2. Handling of Confidential Information

(1) For all information made accessible via the FEV MS Collaboration Environment and derivable from the use of this MS Collaboration Environment, the confidentiality agreements existing between FEV and the external guest users or their organization shall apply. In this context, the requirements of the project management or the inviting party on the part of FEV shall always be met, in particular with regard to the handling and disclosure of confidential information.

(2) Confidential Information may only be disclosed to other persons or access rights thereto may only be granted to such persons to the extent that this is necessary for the cooperation and performance of the assigned tasks, or a legal basis requires this.

(3) Confidential information exchanged in the course of collaborative work may be stored in the FEV MS Collaboration Environment exclusively in the storage location provided for this purpose.

3. Passwords

(1) Passwords (including PINs and passphrases) must be kept secret and may only be entered unobserved. The obligation of secrecy also applies towards employees of FEV and your organization. Passwords may not be stored in plain text or on programmable function keys.

(2) A password must be changed immediately if it has become known to unauthorized persons or if there is a suspicion that this is the case. After a password change, the prior changed password may no longer be used. If a password change is no longer possible to protect system access, the project manager/your contact person in the FEV department must be informed immediately.

(3) Passwords for access to the FEV MS Collaboration Environment or other Microsoft 365 components may not be used more than once for other purposes.

4. Protection of Information Against Unauthorized Access

(1) Personal data and other confidential information shall always be treated confidentially in connection with the use of guest access to the FEV MS Collaboration Environment and shall be

protected against unauthorized access. This includes, but is not limited to, the alignment or shielding of screens to prevent unauthorized viewing, the use of password-protected screen locks even in case of a short-term absence, the logout from the FEV MS Collaboration Environment after the end of a work session and the activation of effective access locks on the end device used as well as the prompt installation of updates (in particular security updates and virus definitions).

(2) The protection of confidential information shall be ensured by the guest user at all times, regardless of the terminal device used to access the Collaboration Environment. However, the use of the FEV MS Collaboration Environment via mobile end devices such as notebooks, smartphones and tablets require special caution. If a mobile end device is lost, the project manager/your contact person in the FEV department shall be informed immediately if there is a risk that access or other confidential data of FEV could thereby become accessible to unauthorized persons.

(3) The applicable requirements of the organization of the guest user, if any, shall remain unaffected.

5. Exclusively Business/Project-related Use

Access to the FEV MS Collaboration Environment is provided to guest users solely for collaboration within the framework of FEV business purposes and those of its business partners. Use for private purposes is not permitted.

6. Data Protection Violations

If a guest user becomes aware of or suspects a data breach, they shall immediately inform their contact person at FEV. The same applies to the suspicion that a file or data carrier is infected with malware or otherwise compromised.

7. Teams Conferences

(1) For all members of a Teams Conference, there must be mutual transparency with regard to the identity of the participants. It is therefore prohibited in particular to provide personal access data to other persons or otherwise allow other persons to participate in a Teams conference unrecognized or unidentified. .

(2) The use of the camera function during participation in Teams conferences is voluntary. Image and sound recordings may only be made in exceptional cases and only with the prior consent of all participants involved and only by FEV. Providing recordings to persons outside the circle of participants in the Teams conference also requires the documented consent of all participants.

8. Prohibited Communication Purposes/Contents/Forms

(1) Guest users shall refrain from any use of the FEV MS Collaboration Environment that violates applicable law and/or is likely to harm the interests of FEV or its customers and business partners or to impair the security of FEV's IT systems.

(2) This shall apply in particular to

- the retrieval, uploading or dissemination of content which violates regulations of personal rights, copyright or criminal law and/or of insulting, defamatory, racist, sexist or pornographic content or content which glorifies violence;

- the private use of the MS Collaboration Environment (see above);
- the circumvention of binding regulations or established standards by means of the MS Collaboration Environment;
- the transmission of viruses or other malware.

(3) The relevant terms of use of the Microsoft service agreement for the MS Collaboration Environment of the organization shall be observed.

9. Documentation of Work Results, Availability

FEV assumes no guarantee to guest users regarding the availability of the MS Collaboration Environment by means of the guest accesses or the documentation of work results in it.

10. Compliance with Data Protection Principles

Guest users shall, to the extent of their ability, contribute to ensuring the following data protection principles by complying with this Terms of use and, if applicable, the requirements of their organization:

- **Lawfulness, Fairness, and Transparency:** Personal data must be processed in a lawful and fair manner and in a way that is comprehensible to the data subject. In the context of collaboration, personal data may therefore in principle only be exchanged to the extent that this is necessary for the performance of the official tasks of the communication participants within the context of the project work.
- **Purpose limitation:** Personal data must be collected for specified, explicit and legitimate purposes and must not be further processed in a manner incompatible with those purposes. A clear, legitimate purpose for processing personal data as part of the collaborative work must exist and the processing of the data must always be compatible with that purpose.
- **Data minimization:** Personal data must be adequate and relevant to the purpose and limited to what is necessary for the purposes of the processing. Guest users may therefore process only the personal data necessary for the purpose of the processing in the context of collaborative work and, wherever possible, process it only in anonymous or pseudonymous form.
- **Accuracy**: Personal data must be accurate and, when necessary, kept up to date. Every reasonable measure must be taken to ensure that personal data which is inaccurate with regard to the purposes for which it was processed is erased or rectified without delay. Guest users may therefore also be required to correct or delete inaccurate or outdated data, or to restrict further processing of this data, or to arrange for this to be done through their respective FEV contact.
- **Integrity and Confidentiality:** Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage by appropriate technical and organizational measures. Appropriate data security must be ensured during data processing (see Points 2-5 above for measures relevant to guest users).

11. Violations of this Acceptable Usage Policy

Violations of this Terms of use may result in civil claims by FEV against the violator and/or its organization, if any. In addition, guest users may have their access to the FEV MS Collaboration Environment revoked.

Annex: Definitions

Personal Data: Any information relating to an identified or identifiable natural person (“data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing: Any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Breach: A security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Confidential Information: "Confidential" information is information that is not generally known or readily accessible, either as a whole or in the precise arrangement and composition of its component parts, to persons in the circles that customarily handle that type of information, and is therefore of commercial value, and is the subject of confidentiality measures that are reasonable under the circumstances by its rightful owner, and for which there is a legitimate interest in maintaining confidentiality. For purposes of this Terms of Service, "Confidential Information" includes personally identifiable information.

Title:	Terms of Service for Guest Users for Collaboration in the FEV MS Collaboration Environment
Person responsible for this policy:	Giselle Laoutoumai; laoutoumai@fev.com
Policy ID (if any):	-
Effective Date:	Dec. 2021
Revision date (only in case of revision):	-
Version number:	1.0
Date of next revision:	-