Terms of use for access to Microsoft 365 Information Systems

1. PREAMBLE

1.1 In the course of joint project processing or the execution of supply/service contracts, BUDENHEIM may grant access to its Microsoft 365 information system to individual persons (users) named by project partners or suppliers (partners). This includes, among other things, file sharing (Teams/OneDrive) and access to SharePoint Online.

1.2 As the granting of access is associated with security risks, the following provisions shall apply; additional obligations arising from the General Terms and Conditions of Purchase of BUDENHEIM, from its information security guidelines for suppliers, confidentiality agreements and/or other related contracts shall continue to apply unchanged. The user acknowledges the following provisions and agrees to them without reservation.

2. GRANTING ACCESS TO THE MICROSOFT 365 ENVIRONMENT AND DATA OF BUDENHEIM

2.1 BUDENHEIM grants the user access to its Microsoft 365 information systems and confidential information as part of the joint collaboration.

2.2. Each user registers for this purpose with his personal e-mail address.

2.3. The user shall use the information and IT systems of BUDENHEIM made accessible to him/her exclusively for the fulfillment of his/her tasks in the joint project or for the fulfillment of the underlying contractual relationship. Disclosure to third parties and/or use for other purposes is expressly prohibited.

2.4. BUDENHEIM is entitled to monitor and record every access to its network and information systems and to retain the recording for a period of 90 days.

2.5. BUDENHEIM is entitled to deny or withdraw access to users at any time, in particular if the behavior of the user or the nature of the equipment used poses a risk to the security or integrity of BUDENHEIM's systems.

2.6. The user must inform BUDENHEIM independently and without delay about security-relevant events; such events are in particular but not exclusively:

- if the user has reason to believe that the IT systems of BUDENHEIM and/or the information provided by it have been or are being used inappropriately
- if the user has reason to believe that access data, access cards or the like have been stolen, lost or otherwise become publicly known or accessible to unauthorized persons
- if the user leaves the partner's company or changes his area of responsibility and there is no need for access in the new area of responsibility.

3. DATA PRIVACY INFORMATION

3.1 Only the necessary personal access data (disclosed e-mail address and password hash) and the access logs are stored in the M365 Security & Compliance Center monitoring log.

3.2 The processing of this personal data serves the legitimate interest of BUDENHEIM in securing access and troubleshooting (prevention, detection, investigation, containment and resolution of problems, including security incidents). This data is deleted 90 days after access.

3.3 Further information on the processing of personal data and your rights in this regard, the options for contacting our Data Protection Officer and our Privacy Policy can be found at https://www.budenheim.com/privacy-policy

4. SONSTIGES

4.1. The Chief Information Security Officer (CISO) of BUDENHEIM is available to answer any questions regarding these Terms of Use and/or for a security briefing.

5. ACKNOWLEDGEMENT AND APPROVAL

5.1. The user has taken note of the above regulations and agrees to them.