**Information Security Fact Sheet for Business Partners October 2023**

Diffutherm B.V.has established and operates an information security management system (ISMS for short) with the aim of protecting (personal) information against internal and external, intentional or accidental threats. In order to meet the requirements of information security and data protection, the Contractor undertakes to comply with the following general security measures:

* Confidential treatment of all information that becomes accessible in connection with the activity to be performed. In particular, this information may not be disclosed to any third party or used for any other purpose. The obligation to maintain confidentiality extends beyond the respective cooperation.
* The taking of documents, work results or IT systems outside the business premises of the client is generally not permitted and requires prior written approval.
* Detected security gaps, vulnerabilities and incidents must be reported to the client immediately.
* Staying on site is allowed only in the premises provided for the performance of the activity.
* Exclusive use of hardware and software released or licensed by the client.
* Exclusive use of the communication links approved by the client.
* Use of hardware/software and information exclusively for fulfilling the agreed tasks.
* Exclusive use of data carriers that have been checked for malware.

If there is access or access to IT systems of the client, the following security measures must be observed:

* Access may only take place via the end devices provided in each case and for the agreed purposes and tasks.
* The disclosure or disclosure of user names and passwords to third parties is to be avoided in any case.
* Security settings, e.g. for protection against malware, must not be taken out of operation, bypassed or changed in any other way.
* The connection of own systems to the communication network of the customer is not permitted.
* Use only of the rights assigned within the scope of the agreed activity.
* Use of secure passwords (minimum length of 15 characters and at least three of the following four character types: upper/lower case letters, numbers, special characters).