**Informatiebeveiligingsbrochure voor zakenpartners Oktober 2023**

Diffutherm B.V. heeft een Information Security Management System (ISMS) opgesteld en hanteert dit met als doel (persoons)gegevens te beschermen tegen interne en externe, opzettelijke of onopzettelijke bedreigingen. Om te voldoen aan de eisen van informatiebeveiliging en gegevensbescherming, verplicht de opdrachtnemer zich tot het naleven van de volgende algemene beveiligingsmaatregelen:

* Vertrouwelijke behandeling van alle informatie die toegankelijk wordt in verband met de uit te voeren activiteit. Deze informatie mag in het bijzonder niet worden doorgegeven aan derden of voor andere doeleinden worden gebruikt. De verplichting tot geheimhouding reikt verder dan de respectieve samenwerking.
* Het meenemen van documenten, werkresultaten of IT-systemen buiten de bedrijfslocatie van de Klant is over het algemeen niet toegestaan en vereist voorafgaande schriftelijke toestemming.
* Geïdentificeerde leemten in de beveiliging, kwetsbaarheden en incidenten worden onverwijld aan de Klant gemeld.
* Verblijf ter plaatse is alleen toegestaan in de ruimten die beschikbaar zijn gesteld voor de uitvoering van de activiteit.
* Exclusief gebruik van de hardware en software die door de klant is vrijgegeven of in licentie is gegeven.
* Exclusief gebruik van de door de opdrachtgever vrijgegeven communicatieverbindingen.
* Gebruik van hardware/software en informatie uitsluitend voor het uitvoeren van de overeengekomen taken.
* Gebruik uitsluitend gegevensdragers die zijn gecontroleerd op malware.

Als er toegang is tot de IT-systemen van de klant, moeten de volgende beveiligingsmaatregelen in acht worden genomen:

* Toegang mag alleen plaatsvinden via de in elk geval verstrekte eindapparaten en voor de overeengekomen doeleinden en taken.
* De bekendmaking of openbaarmaking van gebruikersnamen en wachtwoorden aan derden moet in elk geval worden vermeden.
* Beveiligingsinstellingen, bijvoorbeeld voor bescherming tegen malware, mogen niet buiten werking worden gesteld, worden omzeild of op een andere manier worden gewijzigd.
* De aansluiting van eigen systemen op het communicatienetwerk van de Klant is niet toegestaan.
* Gebruik alleen de toegewezen rechten binnen het kader van de overeengekomen activiteit.
* Gebruik van veilige wachtwoorden (minimaal 15 tekens lang en ten minste drie van de volgende vier soorten tekens: hoofdletters/kleine letters, cijfers, speciale tekens).