Het is voor BaseCRM een essentiële prioriteit om in haar producten en diensten een beveiligingsniveau te bereiken dat een adequate bescherming van informatie waarborgt, zodat al haar klanten deze met het volste vertrouwen kunnen gebruiken.

Daarom heeft de directie van BaseCRM een managementsysteem voor informatiebeveiliging (ISMS) vastgesteld en geïmplementeerd waarmee het bedrijf kan waarborgen dat de informatiesystemen en de informatie die zij verwerken en opslaan aan de volgende beginselen voldoen:

- Vertrouwelijkheid: informatie van BaseCRM mag uitsluitend bekend zijn bij bevoegde personen, na identificatie op het juiste moment en via de daarvoor beschikbare middelen.
- Integriteit: informatie van BaseCRM moet volledig, juist en geldig zijn; de inhoud moet overeenkomen met hetgeen de betrokkenen hebben verstrekt, zonder enige manipulatie.
- Beschikbaarheid: informatie van BaseCRM moet te allen tijde toegankelijk en bruikbaar zijn voor bevoegde en geïdentificeerde gebruikers, waarbij het voortbestaan ervan bij iedere voorziene gebeurtenis gewaarborgd is.
- Traceerbaarheid: alle handelingen met informatie van BaseCRM worden ondubbelzinnig gekoppeld aan een persoon of entiteit.
- Authenticiteit: BaseCRM waarborgt dat een entiteit is wie zij beweert te zijn, of waarborgt de bron waaruit de gegevens afkomstig zijn.

De reikwijdte van het ISMS omvat de informatiesystemen die de ontwikkeling, installatie en het onderhoud van de BaseCRM-oplossing ondersteunen.

Het bij BaseCRM geïmplementeerde informatiebeveiligingsmodel is gebaseerd op de internationale norm ISO/IEC 27001:2022 en is vastgelegd in het Algemeen Handboek Informatiebeveiligingsbeleid. Dit handboek en het geheel van beveiligingsbeleidsregels, procedures, instructies en richtlijnen ter bescherming van de informatieactiva van de organisatie tegen interne of externe, opzettelijke of onopzettelijke bedreigingen vormen het Interne Normenkader voor Informatiebeveiliging van BaseCRM.

De directie neemt de verantwoordelijkheid op zich om de passende materiële en personele middelen beschikbaar te stellen voor het vaststellen en implementeren van de organisatorische, technische en controlemaatregelen die nodig zijn om te voldoen aan de informatiebeveiligingseisen die zijn vastgelegd in het Interne Normenkader voor Informatiebeveiliging van BaseCRM.

Het beveiligingsbeleid wordt onderhouden, bijgewerkt en aangepast aan de doelstellingen van BaseCRM en afgestemd op de context van de organisatie en haar risicobeheerstrategie, waarbinnen het ISMS in stand wordt gehouden. Hiervoor is een proces vastgesteld voor de analyse en het beheer van informatiebeveiligingsrisico's.

De directie bevordert een passend niveau van technische deskundigheid door opleiding en bewustmaking van het personeel en verbindt zich ertoe het binnen het bedrijf geïmplementeerde ISMS te evalueren en voortdurend te verbeteren.

De directie verbindt zich ertoe de jaarlijks vastgestelde algemene informatiebeveiligingsdoelstellingen te verwezenlijken en te voldoen aan de wettelijke en regelgevende vereisten die op BaseCRM van toepassing zijn. De door de organisatie vastgestelde algemene beveiligingsdoelstellingen zijn met name:

- Zorgen voor een passende beoordeling, beheersing en behandeling van risico's om de risicokriticiteitsindex geleidelijk te verlagen.
- Het interne normenkader voor informatiebeveiliging onderhouden en voortdurend verbeteren, met daarin de informatiebeveiligingsbeleidsregels en -processen die voor de gehele organisatie verplicht zijn, en controleren of dit normenkader wordt toegepast.
- Een organisatorisch kader en een verdeling van verantwoordelijkheden voor informatiebeveiliging in stand houden, zodat betrokken medewerkers en derden hun verantwoordelijkheden voor informatiebeveiliging kennen en begrijpen en deze verantwoordelijkheden passen bij hun toegewezen functies.
- Informatieactiva beschermen door de meest doeltreffende beheersmaatregelen toe te passen voor het behoud van hun vertrouwelijkheid, integriteit, beschikbaarheid, traceerbaarheid en authenticiteit.
- Waarborgen dat informatiebeveiliging gedurende de gehele levenscyclus (aanschaf, ontwikkeling en onderhoud) een integraal onderdeel vormt van informatiesystemen.
- Zorgen voor een snelle, doeltreffende en passende afhandeling van informatiebeveiligingsincidenten, -gebeurtenissen en -zwakheden.
- De correcte naleving bevorderen van wettelijke, statutaire of contractuele verplichtingen inzake informatiebeveiliging of beveiligingseisen.

Dit beleid wordt gecommuniceerd aan alle betrokkenen binnen de reikwijdte van het ISMS en wordt voor raadpleging beschikbaar gesteld aan belanghebbenden.

Goedgekeurd op 1 december 2025. Revisie 0.0

Ondertekend: de directie