werkt met talent

caparis

Voorwoord raad van bestuur
Caparis beschouwt informatiebeveiliging al jarenlang als een belangrijk issue. Daarbij is het van essentieel belang dat de risico's voor de klant acceptabel moeten zijn en dat maatregelen werkend gemaakt moeten worden zonder dat dit ten koste gaat van de effectiviteit, flexibiliteit en efficiëntie van de dienstverlening. Daarom voert Caparis een beleid dat erop is gericht om de eisen van klanten, relevante wet- en regelgeving, zoals de AVG en de Cyberbeveiligingswet (NIS2), alsmede ISO 27001:2022 na te komen.

Onze ambitie is, binnen het kader van informatiebeveiliging, een open organisatie te zijn, gericht op samenwerking, waarbij informatiebeveiliging zo min mogelijk een belemmering vormt voor de ambitie.

Het begrip informatiebeveiliging
Dit beleid biedt een raamwerk van beleidsuitgangspunten met betrekking tot de beveiliging van de informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld is om de informatievoorziening te beschermen tegen interne en externe bedreigingen.
Het begrip 'informatiebeveiliging' heeft betrekking op:

- Beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Alle betrokken medewerkers hebben een verantwoordelijkheid bij het geven van invulling aan dit beleid. Het niet naleven van dit beleid kan ernstige gevolgen hebben voor de dienstverlening van Caparis aan haar klanten en kan eventueel leiden tot disciplinaire maatregelen.

Reikwijdte van dit beleid
Dit beleid is van toepassing op alle informatie die gecreëerd, ontvangen, verzonden of bewaard wordt in de dienstverlening van Caparis aan klanten en de daarmee samenhangende wettelijke, contractuele verplichtingen en ondersteunende processen.
Het beleid en de uitwerking hiervan gelden voor alle medewerkers van Caparis. Afwijkingen hierop moeten gemeld worden, zodat het managementsysteem continu verbeterd wordt. Daarnaast geldt het beleid ook voor contractanten, die Caparis ondersteunen bij haar dienstverlening aan klanten.
Onlosmakelijk onderdeel van dit beleid zijn interne gedragsregels waaraan ook alle medewerkers, contractanten en stagiaires zich moeten houden. Er wordt zoveel mogelijk gestreefd naar beveiligingsmaatregelen die gebaseerd zijn op logische principes, omdat deze kosteneffectief en duurzaam zijn.

Deze principes zijn:

- Vertrouwelijke gegevens die je niet hebt, hoef je ook niet te beveiligen.
- Niet slepen met vertrouwelijke gegevens.
- Scheiden van gegevens.

Caparis werkt conform ISO 27001 en is daarmee uiteindelijk verantwoordelijk voor het veilig beschikbaar stellen van haar diensten. Caparis stelt haar klanten daarmee in staat om veilig de diensten van Caparis te kunnen gebruiken. Dit ontslaat echter de klant niet van de eindverantwoordelijkheid voor de beveiliging van haar eigen informatievoorziening.

Pijlers onder het beleid

Optimale beheersing

Caparis streeft naar een optimale beheersing van informatiebeveiligingsrisico's. Optimaal betekent voor Caparis een acceptabel risiconiveau tegen aanvaardbare kosten. Beheersmaatregelen worden genomen op basis van een risicobeoordeling. Wij actualiseren ons risicobeeld minimaal jaarlijks.

Bewustwording

Caparis beseft zich dat verhogen van de bewustwording t.a.v. informatiebeveiliging essentieel is in deze context en dat niet alleen kan worden vertrouwd op beschreven procedures. Het gehele management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt.

Commitment

De medewerkers van Caparis - zowel vast als tijdelijk, intern of extern - hebben zich gecommitteerd aan ons informatiebeveiligingsbeleid en onze gedragsregels. Alle medewerkers van Caparis worden getraind in het gebruik van beveiligingsprocedures.

Betrouwbare partners

Caparis werkt samen met betrouwbare partners. Waar noodzakelijk en mogelijk stellen wij eisen t.a.v. informatiebeveiliging aan onze partners. Wij monitoren dat onze vertrouwelijke gegevens bij partners in veilige handen zijn.

Compliance

Het informatiebeveiligingsbeleid van Caparis is in lijn met de relevante landelijke en Europese wet- en regelgeving. Het beleid wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, geregistreerde incidenten en risicoanalyses.

Beleidsuitgangspunten

Met onderstaande kwalitatieve beleidsuitgangspunten verwacht Caparis haar informatiebeveiligingsrisico's te beheersen en tegelijk haar flexibiliteit en efficiëntie bij het uitvoeren van haar werkzaamheden te behouden. De beleidsuitgangspunten vormen de brug tussen de informatiebeveiligingsrisico's en de beheersdoelstellingen en -maatregelen. De beleidsuitgangspunten bieden bovendien het kader voor de raad van bestuur, op welke wijze zij wil dat de informatiebeveiligingsdoelstellingen worden vormgegeven, die passend zijn voor Caparis.

werkt met talent

caparis

Bij de verdere invulling van dit beleid gelden de volgende uitgangspunten:

1. Informatiebeveiliging is een belangrijk bedrijfsrisico voor Caparis. De raad van bestuur stelt daarom het beleid vast, beoordeelt de risico's, stelt de maatregelen vast, stelt voldoende middelen ter beschikking en laat periodiek de werking van het beleid en de naleving van deze maatregelen intern en extern beoordelen om te borgen, dat het IB-managementsysteem blijvend adequaat werkt en waar nodig verbeterd wordt.
2. Caparis conformeert zich m.b.t. de informatiebeveiliging aan de relevante wetgeving en de contractuele afspraken met klanten en business partners.
3. Caparis streeft ernaar om haar dienstverlening aan klanten continu te verbeteren.
4. Caparis heeft Business Continuity hoog in het vaandel staan en heeft een managementsysteem dat bestaat uit een samenhangend stelsel van maatregelen, die zowel preventief, detectief, repressief als correctief werkzaam zijn.
5. De beheersdoelstellingen en beheersmaatregelen van de norm ISO 27001 en de privacyrichtlijnen van de Autoriteit Persoonsgegevens (AP) vormen, voor zover zij bijdragen aan de informatiebeveiliging van Caparis en handhaafbaar zijn, het uitgangspunt voor de te definiëren maatregelen. Dit is vooral een bedrijfseconomische afweging.
6. Caparis beschouwt computercriminaliteit als een ongewenst maatschappelijk probleem en ziet het als haar verantwoordelijkheid om passende maatregelen te nemen om schade ten gevolge van criminele activiteiten zoveel mogelijk te beperken.
7. Vertrouwen is voor Caparis een groot goed en zij hanteert naar medewerkers, klanten, leveranciers en andere stakeholders het wederkerigheidsprincipe. Caparis gaat ervan uit, dat zij afspraken nakomen m.b.t. beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening.
8. Het HRM-beleid is mede gericht op het verbeteren van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening bij medewerkers. Beleidspunten voor informatiebeveiliging zijn voor onze medewerkers vertaald naar een praktische gedragscode.
9. De fysieke en logistieke beveiliging van de gebouwen en de ruimtes daarin zijn zodanig, dat de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en gegevensverwerking inclusief de bedrijfsmiddelen gewaarborgd zijn.
10. Ontwikkeling of aanschaf, installatie en onderhoud van informatie- en communicatiesystemen, alsmede inpassing van nieuwe technologieën, moeten zo nodig met aanvullende maatregelen worden uitgevoerd, dat hiermee geen afbreuk wordt gedaan aan de informatiebeveiliging.

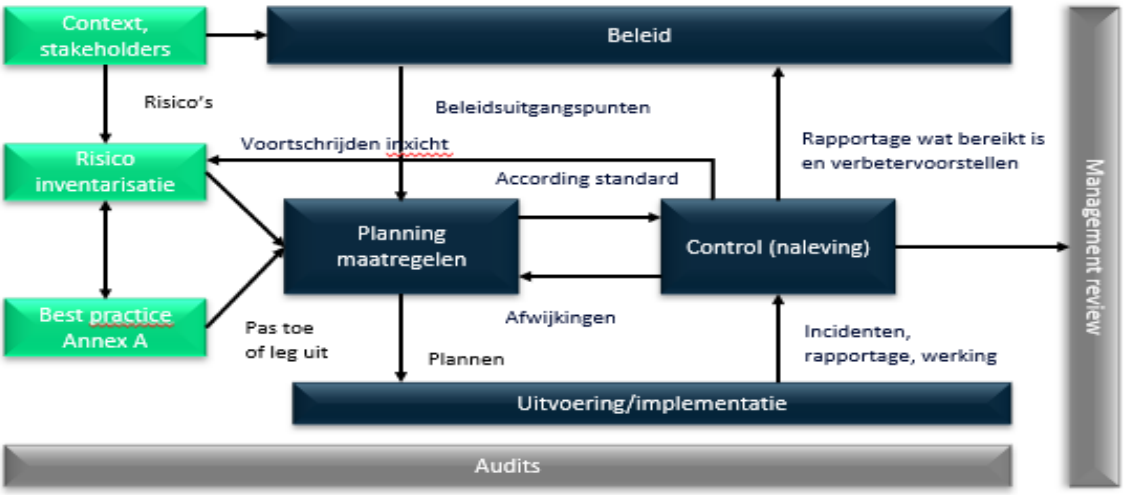
werkt met talent

caparis

11. Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening kan ontstaan.
12. Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten, medewerkers en andere betrokkenen te waarborgen. We hanteren een ‘clear desk’-beleid voor papier en verwijderbare opslagmedia en een ‘clear screen’-beleid voor IT-voorzieningen. Voor het gebruik van ‘User endpoint devices’, zoals laptops en smartphones, zijn afspraken gemaakt.
13. Toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen, gegevensbestanden en programmatuur van Caparis. Ten aanzien van het gebruik van netwerkdiensten is ons uitgangspunt dat gebruikers alleen toegang wordt verleend tot diensten waarvoor ze specifiek bevoegd zijn.
14. Gegevensverstrekking extern gebeurt op basis van 'need to know'. Intern is dit niet altijd wenselijk omdat kennisdeling essentieel is voor een kosteneffectieve dienstverlening aan klanten.
15. Caparis en haar medewerkers treffen maatregelen om te voorkomen, dat vertrouwelijke informatie in handen van derden terechtkomt.
16. Input van klanten die vertrouwelijke data bevat, wordt na verwerking op korte termijn gearchiveerd of vernietigd.
17. Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van deze gegevens.
18. Geautoriseerde medewerkers moeten ook op afstand een beveiligde toegang hebben tot de voor hun relevante productieomgevingen. Er worden geen vertrouwelijke gegevens buiten de productieomgeving opgeslagen. Onder condities kan hiervan afgeweken worden. We hanteren een strikt thuiswerkbeleid.
19. Productieomgevingen zijn gescheiden van andere omgevingen en hierin kunnen specifiek toegangsrechten worden verleend en is monitoring van de toegang mogelijk.
20. Het beheer en de opslag van gegevens in productieomgevingen zijn zodanig, dat geen informatie verloren kan gaan tenzij er sprake is van overmacht.
21. Er zijn functiescheidingen aangebracht tussen de beheer- en gebruikersorganisatie. Verder wordt functiescheiding toegepast waar dat mogelijk en wenselijk is.
22. Er is beleid op het gebied van cryptografische beheersmaatregelen voor de bescherming van informatie. Dit is met name van belang bij informatie-uitwisseling met klanten met een hoog informatiebeveiligingsprofiel.

23. Er is een proces om incidenten adequaat af te handelen en hier 'lessons learned' uit te trekken.
24. Er zijn calamiteitenplannen en -voorzieningen om de beschikbaarheid van de informatievoorziening te waarborgen. We werken met een business continuïteitsplan waarin informatiebeveiliging een belangrijke plaats inneemt.
25. Bij uitbesteding van gegevensverwerking kan de raad van bestuur besluiten om tijdelijk af te wijken van deze beleidsuitgangspunten en de risico's hiervan tijdelijk te accepteren.
26. Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening kan ontstaan.
27. Bij conflicten zoeken wij een oplossing waarin de missie van Caparis wordt gerealiseerd binnen de wettelijke kaders van informatiebeveiliging en privacy.
28. Caparis en haar medewerkers realiseren zich de privacy gevoeligheid van de (bijzondere) persoonsgegevens die zij verwerken en waarborgen te allen tijde de afscherming, corrigeerbaarheid en transparantie van deze gegevens ter bescherming van de persoonlijke levenssfeer van de betrokkenen.

Het Information Security Management System (ISMS)
Dit beleid is uitgewerkt in een Information Security Management System (ISMS) waarin de belangrijkste procedures en andere informatie zijn vastgelegd. Het ISMS is van toepassing op de gehele organisatie, alle processen, informatiesystemen en gegevens(verzamelingen), waarvoor Caparis (risico)verantwoordelijk is. Op basis van dit beleid worden risicoanalyses uitgevoerd en wordt een set van maatregelen gedefinieerd als interne norm, die geldt als minimumniveau van beveiliging voor de dienstverlening aan klanten. In de Verklaring van Toepasselijkheid is vastgelegd welke elementen van de ISO 27001 (Annex A) zijn opgenomen dan wel uitgesloten.
Het ISMS moet borgen dat Caparis blijvend voldoet aan relevante informatiebeveiligingseisen, zoals volgt uit de ISO27001 norm en relevante wet- en regelgeving. Informatiebeveiliging is een continu verbeterproces. Het ISMS kent een 'Plan, do, check en act' cyclus, waardoor continue verbetering en bijsturing mogelijk zijn.



Controle werking en naleving van het beleid
In de 'directiebeoordeling' wordt de werking en de naleving van het beleid intern geëvalueerd en zo nodig aangepast. Jaarlijks wordt een interne audit gehouden. Onderdeel van deze interne audit zijn het opnieuw beoordelen van risico's en een beoordeling van nieuwe contracten en wet- en regelgeving. Onderdeel van deze rapportage is ook een plan met verbetervoorstellen. De directie beoordeelt de rapportage, keurt voorstellen al dan niet goed en kent budget toe voor de realisatie van de voorstellen.
Daarnaast wordt jaarlijks een externe audit uitgevoerd op de werking van het managementsysteem door een onafhankelijke derde partij, die hiertoe bevoegd en deskundig is.

Interne en externe publicatie
Dit beleid is gecommuniceerd aan de medewerkers door middel van plaatsing in Teams/Informatieveiligheid. De beleidsverklaring is vanwege de transparantie geplaatst op de website van Caparis zodat externen hier kennis van kunnen nemen.

Drachten, 1 maart 2026 Voorzitter raad van bestuur

A. Bonnema