					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P01					Documenttitel: **Informatiebeveiligingsbeleid**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

1. Doel

1.1 Dit beleid definieert de overkoepelende inzet van de organisatie voor informatiebeveiliging door de inrichting van een formeel managementsysteem voor informatiebeveiliging (ISMS).

1.2 Het biedt de strategische richting en de basisvereisten voor de bescherming van de vertrouwelijkheid, integriteit, beschikbaarheid en weerbaarheid van alle informatieactiva in fysieke, digitale en cloudomgevingen.

1.3 Dit beleid geeft invulling aan ISO/IEC 27001:2022, clausules 5.2 en 5.1, door de intentie van het leiderschap, de betrokkenheid van het topmanagement en de afstemming van beveiligingsactiviteiten op de organisatiedoelstellingen vast te leggen.

1.4 Het fungeert als het gezaghebbende referentiedocument voor alle onderliggende beleidsdocumenten, normen en procedures binnen het ISMS en is essentieel voor een risicogebaseerde, op naleving gerichte en continu verbeterende beveiligingsomgeving.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle personen, activa en processen die zijn gedefinieerd binnen de reikwijdte van het ISMS, waaronder:

2.1.1 alle bedrijfseenheden, afdelingen, dochterondernemingen en vestigingen

2.1.2 werknemers, opdrachtnemers, tijdelijke medewerkers, consultants en externe dienstverleners

2.1.3 alle gegevens, informatiesystemen, toepassingen, infrastructuur en communicatiekanalen

2.1.4 alle fysieke, cloudgebaseerde, externe en hybride omgevingen waarin bedrijfsgegevens worden verwerkt of geraadpleegd

2.2 Dit beleid is bindend voor alle entiteiten die informatie van de organisatie verwerken en is van toepassing op alle fasen van de informatielevenscyclus, van creatie en verzending tot opslag en vernietiging.

2.3 Uitsluitingen of beperkingen van deze reikwijdte moeten worden gedocumenteerd in de ISMS-scopeverklaring en formeel worden goedgekeurd door het topmanagement.

3. Doelstellingen

3.1 Het inrichten van een ISMS dat in overeenstemming is met ISO/IEC 27001:2022 en risicogebaseerde besluitvorming binnen de gehele organisatie ondersteunt.

3.2 Waarborgen dat de beveiligingsprincipes vertrouwelijkheid, integriteit en beschikbaarheid worden verankerd in alle organisatieactiviteiten, systemen en samenwerkingsrelaties.

3.3 Het mogelijk maken van naleving van wet- en regelgeving en contractuele verplichtingen door meetbare beleidsdoelstellingen voor informatiebeveiliging vast te stellen en te integreren in de bedrijfsvoering.

3.4 Het minimaliseren van de kans op en de impact van informatiebeveiligingsincidenten door middel van doeltreffende preventieve, detectieve en corrigerende beheersmaatregelen.

3.5 Het bevorderen van continue verbetering van de volwassenheid van de informatiebeveiliging aan de hand van gedefinieerde prestatie-indicatoren, audituitkomsten en managementbeoordelingen.

3.6 Het bevorderen van een cultuur van verantwoordingsplicht, bewustwording en weerbaarheid waarin beveiligingsverantwoordelijkheden door al het personeel worden begrepen en uitgevoerd.

4. Rollen en verantwoordelijkheden

4.1 Topmanagement

4.1.1 Keurt het informatiebeveiligingsbeleid en het ISMS-raamwerk goed en onderschrijft deze.

4.1.2 Zorgt voor afstemming tussen beveiligingsdoelstellingen en de bedrijfsstrategie.

4.1.3 Geeft het goede voorbeeld en bevordert een sterke informatiebeveiligingscultuur.

4.1.4 Beoordeelt en keurt belangrijke wijzigingen in de reikwijdte van het ISMS, de risicobehandeling en de governancestructuur goed.

4.2 Chief Information Security Officer (CISO) / ISMS-manager

4.2.1 Is eigenaar van het ISMS en onderhoudt dit beleid in overeenstemming met ISO/IEC 27001.

4.2.2 Geeft leiding aan risicobeoordelingen, de implementatie van beheersmaatregelen en processen voor continue verbetering.

4.2.3 Zorgt voor interfunctionele coördinatie van beveiligingsinspanningen en houdt toezicht op onderliggende beleidsdocumenten.

4.2.4 Rapporteert de status van het ISMS, incidenten, auditresultaten en metrieken aan het uitvoerend management.

4.2.5 Zorgt ervoor dat beleidsbeoordelingen en actualiseringen worden uitgevoerd overeenkomstig sectie 9 van dit document.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor herziening en actualisering

9.1 Frequentie van herziening

9.1.1 Dit beleid moet ten minste jaarlijks worden herzien of bij een van de volgende triggers:

9.1.1.1 significante wijzigingen in wettelijke, regelgevende of contractuele verplichtingen

9.1.1.2 materiële wijzigingen in het risicoprofiel van de organisatie

9.1.1.3 uitkomsten van interne of externe audits

9.1.1.4 grote incidenten of het falen van beheersmaatregelen

9.2 Bevoegdheid en proces voor herziening

9.2.1 De CISO of aangewezen ISMS-manager geeft leiding aan het herzieningsproces.

9.2.2 Input voor de herziening moet ten minste het volgende omvatten:

9.2.2.1 resultaten van interne audits

9.2.2.2 trends in risicobeoordelingen

9.2.2.3 wijzigingen in bedrijfsprocessen en technologie

9.2.2.4 prestaties ten opzichte van KPI's en risicodrempels

9.2.3 Alle actualiseringen moeten:

9.2.3.1 onder versiebeheer vallen en worden gedocumenteerd

9.2.3.2 worden goedgekeurd door het topmanagement

9.2.3.3 worden verspreid naar alle betrokken partijen via officiële communicatiekanalen

9.2.3.4 leiden tot de noodzakelijke actualisering van onderliggende beleidsdocumenten, documentatie en training

10. Gerelateerde beleidsdocumenten en samenhang

10.1 Dit basisbeleid houdt rechtstreeks verband met de volgende organisatorische beveiligingsbeleidsdocumenten en raamwerken:

10.1.1 P2 – Beleid inzake governancerollen en verantwoordelijkheden: definieert de governancestructuur en bevoegdheidshiërarchie waarnaar in dit document wordt verwezen.

10.1.2 P3 – Beleid inzake aanvaardbaar gebruik: borgt naleving van gedragsregels en het aanvaardbaar omgaan met informatieactiva.

10.1.3 P4 – Beleid inzake toegangsbeveiliging: operationaliseert toegangsgerelateerde beheersmaatregelen die uit dit overkoepelende beleid voortvloeien.

10.1.4 P6 – Risicobeheerbeleid: biedt de risicogebaseerde context voor de selectie van beheersmaatregelen en de acceptatie van restrisico's.

10.1.5 P33 – Beleid inzake audit- en nalevingsmonitoring: beschrijft hoe interne assurancemechanismen de handhaving van beleid valideren.

10.2 Deze onderlinge afhankelijkheden waarborgen een volledige afstemming en traceerbaarheid binnen het ISMS en ondersteunen uniforme governance voor risico en naleving.

11. Referentienormen en raamwerken

11.1 Dit informatiebeveiligingsbeleid is formeel afgestemd op de volgende normen en raamwerken om volledige naleving, auditgereedheid en verdedigbaarheid ten opzichte van toezichthouders te waarborgen:

11.2 ISO/IEC 27001

11.2.1 Clausule 5.1 – Leiderschap en betrokkenheid: dit beleid toont de betrokkenheid van het topmanagement bij informatiebeveiliging aan en definieert verantwoordelijkheden en toewijzing van middelen voor het ISMS.

11.2.2 Clausule 5.2 – Informatiebeveiligingsbeleid: dit document dient als het formele informatiebeveiligingsbeleid van de organisatie, afgestemd op vastgestelde beveiligingsdoelstellingen, de bedrijfsstrategie en naleving van ISO/IEC 27001.

11.2.3 Clausule 6.1 – Maatregelen voor het aanpakken van risico's en kansen: de in dit beleid opgenomen risicogebaseerde aanpak zorgt ervoor dat beveiligingsmiddelen evenredig aan dreigingen worden ingezet.

11.2.4 Clausule 9.2 – Interne audit en clausule 10 – Verbetering: dit beleid is ingebed in de cyclus van continue verbetering van de organisatie en is onderworpen aan validatie door interne audit.

11.2.5 ISO/IEC 27002:2022 – Beheersmaatregel 5.1: specificeert richtlijnen voor het vaststellen en onderhouden van beveiligingsbeleid. Dit beleid volgt de aanbevelingen van ISO/IEC 27002 voor hiërarchische documentatie, beoordelingscycli en afdwingbaarheid.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Beleid en procedures voor beveiligingsplanning): dit beleid voldoet aan de vereiste om een formeel, organisatiebreed informatiebeveiligingsbeleid op te stellen, te verspreiden en te herzien.

11.3.2 PM-1 tot en met PM-5: behandelt governance op programmaniveau, waaronder rollen voor informatiebeveiliging, toewijzing van middelen, risicostrategie en integratie van beveiligingsplanning in de bedrijfsvoering.

11.4 AVG (Verordening (EU) 2016/679)

11.4.1 Artikel 5(2): handhaaft het verantwoordingsbeginsel. Dit beleid definieert verantwoordelijke partijen en traceerbare handhavingsmaatregelen.

11.4.2 Artikel 24: vereist de implementatie van technische en organisatorische maatregelen, waaronder beleidsdocumenten die op risico zijn afgestemd.

11.4.3 Artikel 32: ondersteunt de implementatie van passende maatregelen om de beveiliging van persoonsgegevens gedurende de gehele levenscyclus te waarborgen.

11.5 EU NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(a): verplicht entiteiten om een gedocumenteerd beveiligingsbeleid te implementeren dat risicobeheer en governance adresseert. Dit beleid voldoet aan die vereiste en ondersteunt bredere cyberweerbaarheid en de bescherming van kritieke infrastructuur.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 5(2): vereist een gedocumenteerd intern beheersingskader voor ICT-risicobeheer. Dit beleid ondersteunt naleving in de financiële sector door rollen, beheersmaatregelen en toezichtfuncties toe te wijzen in lijn met de governanceverwachtingen van DORA.

11.7 COBIT 2019

11.7.1 EDM01 – Inrichting van het governanceraamwerk: dit beleid ondersteunt ondernemingsgovernance door ISMS-rollen, leiderschapsverplichtingen en strategische doelstellingen te definiëren.

11.7.2 APO01 – Managementraamwerk: ondersteunt de inrichting en werking van een gestructureerd ISMS.

11.7.3 APO12 – Risicobeheer: biedt de basis voor governance van informatiebeveiligingsrisico's.

11.7.4 MEA01/MEA03 – Monitoren, evalueren en beoordelen: versterkt continue prestatie-evaluatie en monitoring van interne beheersing door handhaving van beleidsnaleving.