					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P01S					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**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausules 5.1, 5.2, 5.3, 6.1, 6.2, 8	Specificeert managementbetrokkenheid, beleidseisen, toewijzing van rollen, risicobeoordeling en operationele beheersing
ISO/IEC 27002:2022	Beheersmaatregelen 5.1–5	Specificeert het opstellen van gedocumenteerd informatiebeveiligingsbeleid, de toewijzing van rollen, functiescheiding en managementverantwoordelijkheden
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Vereisten voor een informatiebeveiligingsprogramma, planningsbeleid, beoordeling en autorisatie, en toegangsbeveiliging
AVG (EU 2016/679)	Artikel 5(2), Artikel 32	Verantwoordingsplicht en maatregelen voor de beveiliging van verwerking, met name voor gedocumenteerde rollen
NIS2-richtlijn (EU 2022/2555)	Artikel 21(2)(a)	Vereist risicobeheersmaatregelen, rollen en verantwoordelijkheden voor cyberrisico's
DORA (EU 2022/2554)	Artikel 9, Artikel 10	Vereist toewijzing van rollen voor ICT-risicomanagement en bedrijfscontinuïteit
COBIT 2019	EDM03, APO13, DSS05	Borgt risico-optimalisatie, beveiligingsbeheer en beheer van beveiligingsdiensten door middel van duidelijke roltoewijzing

1. Doel

1.1 Dit beleid bevestigt de inzet van onze organisatie voor de bescherming van klant- en bedrijfsinformatie door verantwoordelijkheden en praktische beveiligingsmaatregelen duidelijk vast te leggen, passend voor organisaties zonder eigen IT-afdeling.

1.2 Het waarborgt dat alle medewerkers, contractanten en dienstverleners afdwingbare regels naleven, zodat volledige naleving van de certificeringseisen van ISO/IEC 27001 mogelijk is.

1.3 Dit beleid stelt onze organisatie in staat het vertrouwen van klanten op te bouwen door duidelijk aan te tonen hoe wij hun informatie beschermen via vastgelegde verantwoordelijkheden, gestructureerde processen en aantoonbare verantwoording.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle personen die toegang hebben tot of beheer voeren over de gegevens en systemen van de organisatie, waaronder:

2.1.1 Eigenaren en algemeen directeuren

2.1.2 Medewerkers, contractanten en stagiairs

2.1.3 Externe IT-dienstverleners of adviseurs

2.2 Het beleid heeft betrekking op alle soorten informatie, systemen en diensten, waaronder:

2.2.1 Bedrijfsregistraties, klantgegevens, wachtwoorden en e-mails

2.2.2 IT-hardware zoals laptops en telefoons

2.2.3 Cloudservices die worden gebruikt voor bestandsopslag, communicatie of financiële processen

2.2.4 Fysieke documenten die op kantoorlocaties worden bewaard

2.3 Het beleid geldt voor alle werkomgevingen — op kantoor, op afstand en in de cloud — en omvat alle apparaten en software die worden gebruikt om bedrijfsinformatie te verwerken of op te slaan.

3. Doelstellingen

3.1 Duidelijke verantwoordelijkheid toewijzen: waarborgen dat altijd een verantwoordelijke voor informatiebeveiliging is aangewezen. In de regel is dit de Algemeen directeur (GM) of de persoon die deze formeel aanwijst.

3.2 Klant- en bedrijfsinformatie beschermen: betrouwbare en consistente beveiligingsmaatregelen bieden om misbruik, verlies of diefstal van gevoelige gegevens, waaronder klant- en financiële gegevens, te voorkomen.

3.3 Ondersteuning van ISO/IEC 27001-certificering: de organisatie in staat stellen volledige naleving van de eisen van ISO/IEC 27001 aan te tonen, zodat zij auditgereed is en voor certificering in aanmerking komt zonder complexe infrastructuur.

3.4 Beveiliging verankeren in de bedrijfsvoering: informatiebeveiliging integreren in de dagelijkse werkzaamheden en besluitvorming binnen de organisatie.

3.5 Beveiligingsbewustzijn en -cultuur versterken: iedere medewerker stimuleren om beveiligingspraktijken te begrijpen en na te leven, zoals het gebruik van sterke wachtwoorden en het melden van verdachte activiteiten.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur of bedrijfseigenaar

4.1.1 Draagt de volledige eindverantwoordelijkheid voor informatiebeveiliging.

4.1.2 Keurt dit beleid goed en houdt het actueel.

4.1.3 Zorgt ervoor dat alle belangrijke beveiligingstaken rechtstreeks worden uitgevoerd of schriftelijk worden gedelegeerd.

4.1.4 Verifieert dat gedelegeerde beveiligingstaken, zoals toegangsbeheer of incidentafhandeling, doeltreffend worden uitgevoerd.

4.1.5 Treedt op als standaard aanspreekpunt voor alle interne en externe beveiligingsaangelegenheden, waaronder audits en klantvragen.

4.1.6 Bewaakt tijdens de jaarlijkse beoordeling de voortgang ten opzichte van deze doelstellingen. Doelstellingen moeten waar mogelijk meetbaar zijn (bijvoorbeeld percentage opgeleid personeel, aantal gemelde incidenten) en worden herzien op basis van beveiligingsbevindingen en veranderingen in het risicoprofiel.

4.2 Aangewezen medewerker (indien van toepassing)

4.2.1 Kan de Algemeen directeur ondersteunen bij dagelijkse taken, zoals het aanmaken van gebruikersaccounts, het intrekken van toegang van uitdiensttreders of de afstemming met de IT-dienstverlener.

4.2.2 Moet formeel zijn aangewezen en beschikken over voldoende bevoegdheden en middelen om de taken uit te voeren.

4.2.3 Rapporteert eventuele problemen aan de Algemeen directeur.

[... 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 actualisatie

9.1 Jaarlijkse beoordeling

9.1.1 Dit beleid moet door de Algemeen directeur (GM) ten minste eenmaal per jaar worden beoordeeld om voortdurende naleving van de certificeringseisen van ISO/IEC 27001, wijzigingen in regelgeving (zoals de AVG, NIS2 en DORA) en veranderende bedrijfsbehoeften te waarborgen.

9.2 Tussentijdse beoordelingen

9.2.1 Aanvullende beoordelingen moeten plaatsvinden wanneer zich significante wijzigingen voordoen, zoals:

9.2.1.1 Ernstige beveiligingsincidenten of datalekken.

9.2.1.2 Invoering van nieuwe bedrijfsprocessen of technologieën (bijvoorbeeld nieuwe software, platforms voor werken op afstand of cloudservices).

9.2.1.3 Wijzigingen in wettelijke of regelgevende vereisten die van invloed zijn op de verwerking van informatie.

9.3 Documentatie van wijzigingen

9.3.1 Alle beleidsbeoordelingen en wijzigingen moeten formeel worden gedocumenteerd, met duidelijke vermelding van de datum, de aard van de wijzigingen en de goedkeuring door de GM.

9.3.2 Een historisch overzicht van beleidsversies moet veilig worden bewaard om de ontwikkeling van het beleid en de naleving tijdens audits aan te tonen.

9.4 Communicatie van actualisaties

9.4.1 Wijzigingen in dit beleid moeten tijdig worden gecommuniceerd aan alle medewerkers, contractanten en relevante derden.

9.4.2 Geactualiseerde versies van het beleid moeten eenvoudig toegankelijk zijn voor alle betrokken medewerkers (bijvoorbeeld elektronisch gedeeld of fysiek op de werkplek beschikbaar gesteld).

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid hangt nauw samen met andere beleidslijnen binnen de SME-beleidsset van de organisatie, in het bijzonder:

10.1.1 P2S – Beleid inzake governance, rollen en verantwoordelijkheden: verduidelijkt de toewijzing van beveiligingstaken en verantwoordelijkheden.

10.1.2 P4S – Toegangscontrolebeleid: definieert de veilige omgang met toegang tot bedrijfsinformatie.

10.1.3 P8S – Beleid voor informatiebeveiligingsbewustzijn en opleiding: biedt essentiële richtlijnen voor training en bewustwording van medewerkers.

10.1.4 P17S – Beleid inzake gegevensbescherming en privacy: waarborgt naleving van de AVG en andere wetgeving inzake gegevensbescherming.

10.1.5 P30S – Incidentresponsbeleid: beschrijft de gedetailleerde acties die nodig zijn in reactie op beveiligingsincidenten.

10.2 Deze gekoppelde beleidslijnen bieden duidelijke operationele richtlijnen en moeten gezamenlijk worden geïmplementeerd om volledige naleving voor ISO/IEC 27001-certificering te bereiken.

11. Referentienormen en -kaders

11.1 ISO/IEC 27001

11.1.1 Clausule 5.1 – Leiderschap en betrokkenheid: vereist betrokkenheid van het topmanagement en verantwoording voor de doeltreffendheid van informatiebeveiliging binnen de organisatie.

11.1.2 Clausule 5.2 – Informatiebeveiligingsbeleid: schrijft duidelijke, gedocumenteerde beleidslijnen voor die zijn afgestemd op de organisatiestrategie en nalevingsverplichtingen.

11.1.3 Clausule 5.3 – Organisatorische rollen en verantwoordelijkheden: definieert een duidelijke toewijzing van verantwoordelijkheden voor informatiebeveiliging binnen de organisatie, essentieel voor doeltreffende informatiebeveiligingsgovernance en auditnaleving.

11.1.4 Clausule 6.1 – Acties om risico's en kansen aan te pakken: waarborgt dat informatiebeveiligingsrisico's systematisch worden geïdentificeerd, beoordeeld en behandeld.

11.1.5 Clausule 8.1 – Operationele planning en beheersing: vereist dat de organisatie de processen plant en implementeert die nodig zijn om informatiebeveiligingsdoelstellingen te behalen en bijbehorende risico's doeltreffend te beheersen.

11.2 ISO/IEC 27002:2022 Beheersmaatregelen 5.1–5

11.2.1 Bijlage A Beheersmaatregel 5.1 – Beleid voor informatiebeveiliging: specificeert het opstellen en communiceren van gedocumenteerde beleidslijnen voor informatiebeveiliging.

11.2.2 Bijlage A Beheersmaatregel 5.2 – Rollen voor informatiebeveiliging: verduidelijkt en wijst formeel rollen en verantwoordelijkheden voor informatiebeveiliging toe aan relevante partijen.

11.2.3 Bijlage A Beheersmaatregel 5.3 – Functiescheiding (SoD): vereist duidelijke functiescheiding om belangenconflicten en frauderisico's bij het beheren van gevoelige informatie te beperken.

11.2.4 Bijlage A Beheersmaatregel 5.4 – Verantwoordelijkheden van het management: schrijft voor dat het management betrokkenheid bij informatiebeveiliging aantoont door actief toezicht en toewijzing van middelen.

11.2.5 Versterkt de noodzaak van duidelijk gedocumenteerde beleidslijnen, rollen, verantwoordelijkheden en governancestructuren voor informatiebeveiliging, zodat consistent beheer en audittraceerbaarheid binnen de organisatie zijn gewaarborgd.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Plan voor het informatiebeveiligingsprogramma: vereist gedocumenteerde strategieën en beleidslijnen voor informatiebeveiligingsgovernance en biedt een kader voor consistente implementatie en beheersing.

11.3.2 PL-1 – Beleid voor beveiligingsplanning: schrijft een organisatiebreed beleid voor beveiligingsplanning voor om veilige bedrijfsvoering en strategische afstemming van informatiebeveiligingsactiviteiten te ondersteunen.

11.3.3 CA-1 – Beleid voor beveiligingsbeoordeling en -autorisatie: vereist duidelijk gedefinieerde rollen voor beoordeling en autorisatie om blijvende doeltreffendheid en naleving van informatiebeveiligingsvereisten te waarborgen.

11.3.4 AC-1 – Beleid inzake toegangsbeveiliging: vereist dat organisaties praktijken en verantwoordelijkheden voor toegangsbeheer duidelijk definiëren, documenteren en afdwingen.

11.4 AVG (EU 2016/679)

11.4.1 Artikel 5(2) – Verantwoordingsplicht: vereist dat organisaties naleving van beginselen inzake gegevensbescherming aantonen, inclusief gedocumenteerde rollen en beleidslijnen voor verantwoordelijkheden op het gebied van gegevensbescherming.

11.4.2 Artikel 32 – Beveiliging van verwerking: schrijft passende technische en organisatorische maatregelen voor, inclusief duidelijke beveiligingsverantwoordelijkheden, om persoonsgegevens te beschermen tegen inbreuken en ongeautoriseerde toegang.

11.5 NIS2-richtlijn (EU 2022/2555)

11.5.1 Artikel 21(2)(a) – Risicobeheersmaatregelen: vereist duidelijke governance-inrichting, inclusief vastgelegde rollen en verantwoordelijkheden voor informatiebeveiliging, die essentieel zijn om cyberrisico's doeltreffend te beheersen.

11.6 DORA (EU 2022/2554)

11.6.1 Artikel 9 – ICT-risicomanagement: vereist dat organisaties rollen en verantwoordelijkheden met betrekking tot ICT-risicomanagement duidelijk toewijzen, ter versterking van weerbaarheid en paraatheid voor bedrijfscontinuïteit.

11.6.2 Artikel 10 – ICT-bedrijfscontinuïteit: vereist duidelijke verantwoording en gestructureerde rollen voor het in stand houden van ICT-weerbaarheid en continuïteit, zodat organisaties betrouwbaar kunnen reageren op verstoringen.

11.7 COBIT 2019

11.7.1 EDM03 – Zorgdragen voor risico-optimalisatie: benadrukt duidelijk gedefinieerde verantwoording en rollen bij het beheren van organisatierisico's en ondersteunt sterke governance en doeltreffend toezicht op informatiebeveiligingsrisico's.

11.7.2 APO13 – Beveiliging beheren: vereist dat organisaties verantwoordelijkheden voor beveiligingsbeheer duidelijk vaststellen en communiceren, zodat afstemming met bedrijfsdoelstellingen en regelgevende vereisten wordt gewaarborgd.

11.7.3 DSS05 – Beveiligingsdiensten beheren: vraagt om gestructureerde rollen en duidelijke verantwoordelijkheden bij het beheren van beveiligingsdiensten, zodat consistente implementatie en verificatie van naleving mogelijk zijn.