					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P02S					Documenttitel: **Beleid inzake governancerollen en -verantwoordelijkheden**						
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	Clausule 5	
ISO/IEC 27002:2022	Beheersmaatregelen 5.2, 5.3, 5.4	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
AVG	Artikelen 5(2), 32	

1. Doel

1.1 Dit beleid bepaalt hoe governancerollen en verantwoordelijkheden voor informatiebeveiliging binnen de organisatie worden toegewezen, gedelegeerd en beheerd, teneinde volledige naleving van ISO/IEC 27001:2022 en andere complianceverplichtingen te waarborgen.

1.2 Dit beleid borgt verantwoording op elk niveau en ondersteunt de operationele doeltreffendheid door duidelijk vast te leggen wie verantwoordelijk is voor elke beveiligingsgerelateerde functie.

1.3 Dit beleid draagt bij aan auditgereedheid en versterkt het vertrouwen van klanten door formele informatiebeveiligingsgovernance aantoonbaar te maken, ook in organisaties met beperkte technische capaciteit of uitbestede IT.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle personen die systemen of gegevens van de organisatie verwerken, waaronder:

2.1.1 bedrijfseigenaren en algemeen directeuren

2.1.2 werknemers en contractanten

2.1.3 externe IT-dienstverleners of consultants

2.2 Dit beleid geldt voor alle systemen, omgevingen en diensten die worden gebruikt voor het verwerken, verzenden of opslaan van bedrijfs- of klantinformatie, waaronder:

2.2.1 kantoor-IT-infrastructuur en voorzieningen voor werken op afstand

2.2.2 cloudplatforms en e-maildiensten

2.2.3 fysieke registraties en gedeelde schijven

2.3 De reikwijdte omvat zowel interne als uitbestede activiteiten op het gebied van informatiebeveiligingsgovernance.

3. Doelstellingen

3.1 Het vaststellen van duidelijke verantwoording voor alle beveiligingsgerelateerde taken, waaronder beleidsbeheer, toegangsbeheer, incidentrespons en monitoring.

3.2 Het mogelijk maken van effectieve functiescheiding (SoD) om belangenconflicten en frauderisico's te beperken.

3.3 Het waarborgen dat beveiligingstaken en rollen duidelijk worden gedocumenteerd en periodiek worden herzien.

3.4 Het mogelijk maken van onderbouwde besluitvorming, escalatie en toezicht op IT- en beveiligingsrisico's.

3.5 Het ondersteunen van certificering volgens ISO/IEC 27001:2022 en het versterken van vertrouwen bij klanten, partners en auditors.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur / bedrijfseigenaar

4.1.1 Draagt de eindverantwoordelijkheid voor de implementatie van en het toezicht op dit beleid.

4.1.2 Keurt alle beveiligingsrollen, verantwoordelijkheden en delegatiebesluiten goed.

4.1.3 Ziet toe op naleving en neemt eindbesluiten over beleidsuitzonderingen en escalaties.

4.2 Aangewezen beveiligingscoördinator (indien van toepassing)

4.2.1 Deze rol kan worden vervuld door een medewerker of een vertrouwde consultant.

4.2.2 In micro-ondernemingen kan deze rol worden vervuld door de algemeen directeur of een externe dienstverlener.

4.2.3 Ondersteunt de dagelijkse uitvoering van toegangsbeheer, incidentrespons en elementaire technische beveiligingstaken.

4.2.4 Rapporteert rechtstreeks aan de algemeen directeur over beveiligingskwesties of risico's.

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

9. Vereisten voor herziening en actualisering

9.1 Jaarlijkse herziening

9.1.1 Dit beleid moet elke 12 maanden door de algemeen directeur worden herzien om te waarborgen dat het in lijn blijft met wettelijke verplichtingen, operationele behoeften en vereisten voor ISO/IEC 27001-certificering.

9.2 Tussentijdse herzieningen

9.2.1 Herzieningen moeten ook plaatsvinden wanneer:

9.2.1.1 zich belangrijke organisatorische wijzigingen voordoen

9.2.1.2 een nieuwe dienstverlener wordt gecontracteerd

9.2.1.3 zich een ernstig beveiligingsincident voordoet

9.2.1.4 regelgeving zoals de AVG, NIS2 of DORA wordt bijgewerkt

9.3 Versiebeheer en documentatie

9.3.1 Alle herzieningen moeten bevatten:

9.3.1.1 datum van herziening

9.3.1.2 samenvatting van eventuele wijzigingen

9.3.1.3 handtekening van of gedocumenteerde goedkeuring door de algemeen directeur

9.3.1.4 gearchiveerde eerdere versies als auditreferentie

9.4 Communicatie van wijzigingen

9.4.1 Alle beleidswijzigingen moeten tijdig aan medewerkers en dienstverleners worden gecommuniceerd via e-mail, interne portalen of formele memo's.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid moet in samenhang met de volgende SME-beleidslijnen worden geïmplementeerd om volledige doeltreffendheid te waarborgen:

10.1.1 P4S – Beleid inzake toegangscontrole: bepaalt hoe toegang wordt verleend, beheerd en ingetrokken, en is direct gekoppeld aan toegewezen rollen en toezicht.

10.1.2 P8S – Beleid inzake informatiebeveiligingsbewustzijn en opleiding: versterkt rolspecifieke verantwoordelijkheden en verwachtingen.

10.1.3 P17S – Beleid inzake gegevensbescherming en privacy: beschrijft wettelijke verplichtingen onder de AVG, die worden toegewezen aan rollen die in dit governancebeleid zijn gedefinieerd.

10.1.4 P30S – Incidentresponsbeleid: vereist vastgelegde verantwoordelijkheden voor melding, escalatie en afhandeling van incidenten.

10.2 Deze beleidslijnen maken gezamenlijk consistente handhaving, interne verantwoording en externe naleving mogelijk.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 5.3 – Organisatorische rollen, verantwoordelijkheden en bevoegdheden: vereist dat rollen duidelijk worden toegewezen en ondersteund door het topmanagement.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregelen 5.2–5.4: vereisen duidelijke documentatie van rollen op het gebied van informatiebeveiliging, functiescheiding en managementtoezicht.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: stelt een overkoepelend informatiebeveiligingsprogramma vast met gedefinieerde verantwoordelijkheden.

11.3.2 PL-1 tot en met PL-4: vereisen planningsmaatregelen, waaronder beleidsformulering en gedocumenteerde roltoewijzingen.

11.3.3 CA-1: vereist vastgelegde rollen voor beoordeling en autorisatie.

11.3.4 AC-1: koppelt rolgebaseerde toegangscontrole aan toegewezen governanceverantwoordelijkheden.

11.4 AVG

11.4.1 Artikel 5(2) – Verantwoordingsplicht: vereist dat organisaties naleving aantoonbaar maken door middel van rollen en verantwoordelijkheden.

11.4.2 Artikel 32 – Beveiliging van de verwerking: benadrukt een duidelijke toewijzing van taken ter bescherming van persoonsgegevens.

11.5 EU NIS

11.5.1 Artikel 21(2)(a): vereist governancestructuren met geformaliseerde rollen voor het beheersen van cyberrisico's en incidenten.

11.6 EU DORA

11.6.1 Artikelen 9 en 10: vereisen dat financiële entiteiten ICT- en beveiligingsgerelateerde verantwoordelijkheden duidelijk toewijzen en daarop toezicht houden.

11.7 COBIT 2019

11.7.1 EDM03 – Zorgdragen voor risico-optimalisatie: vereist duidelijk gedefinieerde rollen en escalatieroutes voor het beheersen van beveiligingsrisico's.

11.7.2 APO13 – Beveiliging beheren: wijst strategische en operationele beveiligingstaken toe aan personen en rollen.

11.7.3 DSS05 – Beveiligingsdiensten beheren: vereist structuur en herleidbaarheid in verantwoordelijkheden voor externe en interne beveiligingsdiensten.