					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P02					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 5.3; Bijlage A, beheersmaatregel 5	
ISO/IEC 27002:2022	Beheersmaatregel 5	
NIST SP 800-53 Rev.5	PL-1 tot en met PL-4, PM-1 tot en met PM-13	
AVG	Artikelen 5(1)(f), 24, 37	
EU NIS2	Artikel 21(2)(a)	
EU DORA	Artikel 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Doel

1.1 Dit beleid definieert het governancemodel, de organisatierollen en de verantwoordelijkheden die nodig zijn voor een doeltreffende werking van het managementsysteem voor informatiebeveiliging (ISMS).

1.2 Het legt duidelijke lijnen vast voor verantwoordingsplicht, beslissingsbevoegdheid en escalatie om te waarborgen dat informatiebeveiliging op alle niveaus van de organisatie is verankerd en is afgestemd op de strategische bedrijfsdoelstellingen.

1.3 Dit beleid geeft invulling aan de vereisten van ISO/IEC 27001:2022, clausule 5.3 en beheersmaatregel A.5.2, en waarborgt dat verantwoordelijkheden voor beveiligingsgerelateerde activiteiten duidelijk worden toegewezen, gedocumenteerd, gecommuniceerd en periodiek beoordeeld.

1.4 Dit beleid biedt tevens een basis voor geïntegreerde governance met andere disciplines, zoals risicomanagement, compliance, IT-operaties en juridische zaken.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle personen en entiteiten die betrokken zijn bij de governance, uitvoering en het toezicht op informatiebeveiliging binnen de reikwijdte van het ISMS. Dit omvat:

2.1.1 uitvoerend management, hoger management en bestuursleden

2.1.2 ISMS-managers, CISO's en beheersmaatregeleigenaren

2.1.3 proceseigenaren en asset-eigenaren

2.1.4 contractanten en externe dienstverleners met gedelegeerde beveiligingsverantwoordelijkheden

2.2 Dit beleid heeft betrekking op zowel interne functies als uitbestede functies (bijvoorbeeld een uitbesteed SOC of beheerders van cloudplatforms) wanneer governancerollen formeel zijn toegewezen of contractueel zijn vastgelegd.

2.3 Dit beleid is tevens van toepassing op organisatieonderdelen, afdelingen en projectteams die beveiligingsrelevante activa, systemen of diensten beheren of beïnvloeden.

3. Doelstellingen

3.1 Waarborgen dat rollen en verantwoordelijkheden op het gebied van informatiebeveiliging formeel zijn gedefinieerd, toegewezen, gecommuniceerd en gedocumenteerd.

3.2 Een governancemodel in stand houden dat functiescheiding (SoD) afdwingt, belangenconflicten voorkomt en escalatie van onopgeloste beveiligingskwesties mogelijk maakt.

3.3 Waarborgen dat verantwoordingsplicht en bevoegdheden voor beveiligingsbeslissingen worden belegd in lijn met de impact op de bedrijfsvoering en de organisatiestructuur.

3.4 Een kader vaststellen voor het beheren van delegaties, rolwijzigingen en de beoordeling van toegewezen verantwoordelijkheden.

3.5 Assurance bieden aan belanghebbenden, waaronder toezichthouders, auditors en klanten, dat informatiebeveiliging doeltreffend wordt aangestuurd en in overeenstemming is met toepasselijke normen.

4. Rollen en verantwoordelijkheden

4.1 Uitvoerend management (topmanagement)

4.1.1 Biedt strategisch toezicht, stelt middelen beschikbaar en waarborgt afstemming tussen ISMS-doelstellingen en bedrijfsdoelstellingen.

4.1.2 Keurt belangrijke ISMS-documentatie goed, waaronder het informatiebeveiligingsbeleid, risicobehandelplannen en besluiten over herstelmaatregelen.

4.1.3 Neemt deel aan managementbeoordelingen van het ISMS en escaleert besluiten waarvoor goedkeuring op bestuursniveau is vereist.

4.1.4 Bevordert een beveiligingscultuur en stimuleert naleving van de beginselen van informatiebeveiligingsgovernance binnen de organisatie.

4.2 Stuurgroep Informatiebeveiliging (ISSC)

4.2.1 Fungeert als interdisciplinaire governancecommissie voor het toezicht op het ISMS.

4.2.2 Beoordeelt de risicopositie, de effectiviteit van beheersmaatregelen, auditbevindingen en strategische beveiligingsinitiatieven.

4.2.3 Faciliteert afstemming tussen afdelingen (bijvoorbeeld IT, juridische zaken, compliance, HR, risicomanagement en operations).

4.2.4 Keurt escalatiedrempels, budgettoewijzingen en beleidswijzigingen goed waarvoor inbreng van het uitvoerend management vereist is.

[... 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 Beoordelingsschema

9.1.1 Dit beleid moet ten minste jaarlijks worden beoordeeld of wanneer zich een van de volgende situaties voordoet:

9.1.1.1 wijzigingen in de organisatiestructuur of het uitvoerend team

9.1.1.2 uitbreiding of herdefiniëring van de reikwijdte van het ISMS

9.1.1.3 wijzigingen in wet- en regelgeving die van invloed zijn op roltoewijzing of toezicht

9.1.1.4 significante auditbevindingen of incidenten waarbij governancefalen betrokken is

9.2 Beoordelings- en goedkeuringsproces

9.2.1 De ISMS-manager initieert en leidt het beoordelingsproces, inclusief het verzamelen van input van belanghebbenden en feedback uit audits.

9.2.2 Voorgestelde actualisaties moeten worden beoordeeld door de ISSC en formeel worden goedgekeurd door het uitvoerend management.

9.2.3 Elke versie moet worden bijgehouden in het ISMS-documentregister en de volgende metadata bevatten:

9.2.3.1 beleids-ID en titel

9.2.3.2 versienummer en samenvatting van wijzigingen

9.2.3.3 ingangsdatum en datum van de volgende beoordeling

9.2.3.4 beleidseigenaar en goedkeurder

9.2.3.5 classificatieniveau van het document

9.2.3.6 bewaartermijn en archiveringshistorie

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid moet worden gelezen in samenhang met de volgende beleidslijnen:

10.1.1 P1 – Informatiebeveiligingsbeleid: legt het overkoepelende beveiligingsprogramma vast en beschrijft verantwoordelijkheden van het management voor beleidsbekrachtiging en strategisch toezicht.

10.1.2 P5 – Wijzigingsbeheerbeleid: waarborgt dat wijzigingen in governancestructuren, rollen of verantwoordelijkheden worden onderworpen aan gedocumenteerde goedkeuring en risicobeoordeling.

10.1.3 P6 – Risicomanagementbeleid: identificeert en behandelt governancerisico's die voortvloeien uit rolconflicten, niet-toegewezen taken of het ontbreken van escalatie.

10.1.4 P7 – Onboarding- en offboardingbeleid: borgt processen voor de toewijzing van beheersmaatregelen en de intrekking van toegangsrechten bij wijzigingen in de personeelslevenscyclus.

10.1.5 P33 – Beleid inzake audit- en compliancemonitoring: ondersteunt onafhankelijke beoordeling van de effectiviteit van governance en borgt corrigerende maatregelen bij niet-naleving.

10.2 Deze beleidslijnen ondersteunen gezamenlijk een uniform en afdwingbaar ISMS-governancekader.

11. Referentienormen en raamwerken

11.1 Dit beleid is afgestemd op wereldwijd erkende normen en raamwerken voor informatiebeveiligingsgovernance en verantwoordingsplicht ten aanzien van rollen. Het waarborgt herleidbaarheid naar wettelijke, regelgevende en certificeringseisen en ondersteunt een verdedigbare ISMS-structuur.

11.2 ISO/IEC 27001

11.2.1 Clausule 5.3 – Organisatierollen, verantwoordelijkheden en bevoegdheden: dit beleid geeft invulling aan de eis dat voor informatiebeveiliging relevante rollen duidelijk worden toegewezen, gecommuniceerd en gedocumenteerd.

11.2.2 Clausule 9.3 – Managementbeoordeling: dit beleid borgt toezicht door het uitvoerend management op ISMS-rollen en governance via kwartaal- en jaarbeoordelingen.

11.2.3 Bijlage A, beheersmaatregel 5.2 – Rollen en verantwoordelijkheden inzake informatiebeveiliging: definieert rollen op technisch, operationeel en strategisch niveau om functiescheiding (SoD), risico-eigenaarschap en herleidbare verantwoordingsplicht te waarborgen.

11.3 ISO/IEC 27002:2022 – Beheersmaatregel 5

11.3.1 Biedt implementatierichtlijnen voor het toewijzen van verantwoordelijkheden voor informatiebeveiliging binnen een organisatie. Dit beleid volgt deze richtlijnen door roltypen, delegatieregels, escalatieprocedures en beoordelingsmechanismen te definiëren.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 tot en met PL-4: benadrukken de noodzaak van formele planningsdocumentatie, waaronder beleidslijnen die governance definiëren en beveiligingsverantwoordelijkheden toewijzen.

11.4.2 PM-1 (Information Security Program Plan) en PM-2 (Senior Information Security Officer): komen in dit beleid tot uitdrukking via de toewijzing van de CISO/ISMS-manager en formele governancerollen.

11.4.3 PM-5 tot en met PM-13: dit beleid voldoet aan vereisten voor roldocumentatie, organisatiebrede risicorollen, toezicht op configuratiebeheer en integratie met missie- en bedrijfsfuncties.

11.5 AVG (Verordening (EU) 2016/679)

11.5.1 Artikel 5(1)(f): vereist dat persoonsgegevens worden beschermd tegen ongeautoriseerde of onrechtmatige verwerking. Dit beleid waarborgt dat personen met verantwoordelijkheden voor gegevensbescherming duidelijk worden aangewezen en geregistreerd.

11.5.2 Artikel 24: vereist passende organisatorische maatregelen, waaronder governancestructuren.

11.5.3 Artikel 37: vereist de aanwijzing van een functionaris voor gegevensbescherming (FG), wat moet zijn weerspiegeld in het governancekader en het register van verantwoordelijkheden van de organisatie.

11.6 EU NIS2-richtlijn (2022/2555)

11.6.1 Artikel 21(2)(a): verplicht entiteiten om beleidslijnen voor risicoanalyse en beveiliging van informatiesystemen te implementeren, inclusief rolspecifieke verantwoordelijkheden. Dit beleid definieert dergelijke rollen en de bijbehorende governancemechanismen.

11.7 EU DORA (2022/2554)

11.7.1 Artikel 5 – Governance- en internbeheersingskader: vereist formele toewijzing van verantwoordelijkheden voor ICT-risicomanagement, besluitvormingsrollen en rapportagelijnen. Dit beleid biedt de basis voor governance van beveiligingsgerelateerde rollen in ICT-omgevingen.

11.8 COBIT 2019

11.8.1 EDM01 – Ensured Governance Framework Setting: dit beleid waarborgt dat het ISMS een duidelijk gedefinieerde governancestructuur heeft die is afgestemd op de behoeften van de organisatie.

11.8.2 EDM02 – Ensured Benefits Delivery: stemt rolgebaseerde beveiligingsactiviteiten af op strategische en operationele doelstellingen en waarborgt verantwoordingsplicht en meetbare resultaten.

11.8.3 APO01 – Managed I&T Management Framework en APO12 – Managed Risk: dit beleid ondersteunt gestructureerd beheer van rollen voor informatiebeveiliging binnen een breder IT-governance- en risicokader.

11.8.4 MEA01 – Monitor, Evaluate and Assess Performance: verankert beoordelingsmechanismen om te verifiëren dat governancerollen doeltreffend, actueel en afdwingbaar zijn.