					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P06S					Documenttitel: **Beleid inzake risicobeheer**							
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 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 tot en met RA-7, PM-9	
EU NIS2	Artikel 21(2)(a–d)	
EU DORA	Artikel 5	
COBIT 2019	APO12, MEA01	

1. Doel

1.1 Dit beleid bepaalt hoe de organisatie risico's identificeert, beoordeelt en beheerst met betrekking tot informatiebeveiliging, bedrijfsvoering, technologie en diensten van derden.

1.2 Het waarborgt dat informatiebeveiligingsrisicobeheer een integraal onderdeel is van planning, projectuitvoering, leveranciersselectie en incidentrespons, in overeenstemming met ISO 27001, ISO 31000 en toepasselijke wet- en regelgeving.

1.3 Dit beleid ondersteunt weloverwogen besluitvorming, de bescherming van informatieactiva en de weerbaarheid van kritieke bedrijfsactiviteiten.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 Alle afdelingen, systemen en gebruikers binnen de organisatie

2.1.2 Alle informatie, diensten en activa die intern of via derden worden beheerd

2.1.3 Risicogerelateerde activiteiten, waaronder projectbeoordelingen, systeemupgrades, uitbesteding en naleving van wet- en regelgeving

2.2 Het omvat alle typen risico's, waaronder:

2.2.1 Cyberdreigingen en systeemkwetsbaarheden

2.2.2 Operationele verstoringen en uitval van dienstverlening

2.2.3 Juridische, compliance- en reputatierisico's

2.2.4 Derdenrisico's en risico's in de toeleveringsketen

2.3 Alle medewerkers, contractanten en dienstverleners moeten dit beleid naleven bij het identificeren of melden van risico's.

3. Doelstellingen

3.1 Eenduidige en herhaalbare procedures voor risicobeoordeling integreren in de reguliere bedrijfsvoering.

3.2 Risico's identificeren en prioriteren die gevolgen kunnen hebben voor vertrouwelijkheid, integriteit, beschikbaarheid of juridische naleving.

3.3 Eigenaarschap toewijzen en beheersmaatregelen vaststellen voor alle significante risico's.

3.4 Een accuraat en actueel risicoregister bijhouden ter ondersteuning van auditgereedheid en risico-opvolging.

3.5 Betrokkenheid van het management waarborgen bij de goedkeuring van risicotolerantie en belangrijke behandelplannen.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur

4.1.1 Stelt de risicobereidheid van de organisatie vast en bekrachtigt het risicobeheerkader.

4.1.2 Keurt belangrijke besluiten over risicobehandeling en de inzet van middelen goed.

4.1.3 Beoordeelt de belangrijkste risico's elk kwartaal samen met de risicocoördinator.

4.2 Risicocoördinator (of ISMS-eigenaar)

4.2.1 Faciliteert risicobeoordelingen en beheert het risicoregister.

4.2.2 Waarborgt dat risicoscores, eigenaarschap en behandelingsmaatregelen worden gedocumenteerd.

4.2.3 Organiseert ten minste eenmaal per jaar een formele risicobeoordeling.

[... 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 actualisatie

9.1 Jaarlijkse beleidsbeoordeling

9.1.1 Dit beleid moet ten minste eenmaal per jaar worden beoordeeld door de algemeen directeur en de risicocoördinator om de relevantie en volledigheid te waarborgen.

9.2 Triggers voor actualisatie

9.2.1 Een tussentijdse beoordeling en actualisatie moet plaatsvinden indien:

9.2.1.1 Een ernstig incident of auditbevinding hiaten in het risicobeheer blootlegt

9.2.1.2 Nieuwe bedrijfseenheden, technologieën of samenwerkingsverbanden worden geïntroduceerd

9.2.1.3 Een wettelijke, regelgevende of contractuele vereiste wijzigt

9.3 Versiebeheer

9.3.1 Alle actualisaties van dit beleid moeten onder versiebeheer plaatsvinden met de volgende metadata:

9.3.1.1 Versienummer en ingangsdatum

9.3.1.2 Samenvatting van wijzigingen

9.3.1.3 Goedkeurder (algemeen directeur)

9.3.1.4 Gearchiveerde voorgaande versies voor auditdoeleinden

9.4 Communicatie en bewustwording

9.4.1 Bijgewerkte versies van het beleid en belangrijke risicobehandelplannen moeten worden gecommuniceerd aan betrokken medewerkers. De jaarlijkse opfristraining moet basisprincipes van risicobewustzijn bevatten.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid hangt samen met verschillende andere beleidslijnen om integrale governance voor informatiebeveiliging te waarborgen:

10.1.1 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: bepaalt wie verantwoordelijk is voor risico-eigenaarschap en besluitvorming.

10.1.2 P5S – Wijzigingsbeheerbeleid: vereist een risicobeoordeling voordat technische of proceswijzigingen worden geïmplementeerd.

10.1.3 P17S – Beleid inzake gegevensbescherming en privacy: behandelt regelgevingsrisico's die samenhangen met de verwerking van persoonsgegevens.

10.1.4 P30S – Incidentresponsbeleid: waarborgt dat risicobehandeling wordt voortgezet tijdens en na beveiligingsincidenten.

10.1.5 P33S – Bedrijfscontinuïteitsbeleid: identificeert restrisico's en herstelmaatregelen voor kritieke diensten.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001:

11.1.1 Clausule 6.1 – Stelt een formeel risicobeheerproces en de planning van risicobehandeling vast.

11.1.2 Clausule 6.1.3 – Vereist dat organisaties gedocumenteerde behandelplannen en goedkeuringen bewaren.

11.2 ISO/IEC 27002:

11.2.1 Beheersmaatregelen 5.4, 5.25 – Bieden implementatierichtlijnen voor risico-eigenaarschap, prioritering en levenscyclusbeheer.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 tot en met RA-7 – Definiëren risicobeoordeling, responsstrategieën, documentatie en beoordelingsmechanismen.

11.4 PM-9 – Vereist consistent toezicht op organisatierisico's op managementniveau.

11.5 EU NIS2-richtlijn

11.5.1 Artikel 21(2)(a–d) – Legt verplichte beheersmaatregelen op voor risicobeoordeling, risicobeperking en governance bij essentiële en belangrijke entiteiten.

11.6 EU DORA

11.6.1 Artikel 5 – Vereist dat gereguleerde entiteiten kaders voor ICT-risicobeheer vaststellen en beheren, inclusief identificatie, classificatie en respons.

11.7 COBIT 2019

11.7.1 APO12 – Risicobeheer: integreert risico in strategische en operationele planning.

11.7.2 MEA01 – Monitoren, evalueren en beoordelen: waarborgt de doeltreffendheid en naleving van risicoprocessen en acties.