					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P06					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, 8.32, 10	Kernvereisten voor risico-identificatie en risicobeheer, integratie in wijzigingsbeheer en continue verbetering
ISO/IEC 27005:2024	Volledige methodologie voor de risicolevenscyclus	Volledig risicobeheerproces in lijn met de norm
ISO 31000:2018	Principes en raamwerk voor risicobeheer	Principes voor risicobeheer opgenomen in het raamwerk
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Richtlijnen en structuur voor risicobeoordelingen, gelaagde governancestructuren voor risico's
AVG	Artikelen 24, 25, 32	Risicoprocessen en beheersmaatregelen voor gegevensbescherming
EU NIS2	Artikel 21(2)(a–d)	Verplichtingen inzake risicobeoordeling en beveiligingsbeoordeling
EU DORA	Artikelen 5, 6	ICT-risicobeheer en operationele weerbaarheid
COBIT 2019	APO12, MEA	Structuur en toezicht voor risicobeheer

1. Doel

1.1 Dit beleid stelt een uniform en geformaliseerd raamwerk vast voor het identificeren, analyseren, evalueren, behandelen, monitoren en beoordelen van informatiebeveiligingsrisico's binnen de gehele organisatie.

1.2 Het waarborgt een consistente toepassing van risicogebaseerde principes ter bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid (CIA) van informatieactiva, in lijn met ISO/IEC 27001:2022, clausule 6.1, en ISO 31000:2018.

1.3 Dit beleid verankert het management van informatiebeveiligingsrisico's in de besluitvormingsprocessen van de organisatie om te voldoen aan interne strategische doelstellingen en externe wettelijke en regelgevende vereisten.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle organisatie-eenheden, bedrijfsprocessen, systemen, medewerkers en betrokkenheid van derden die betrokken zijn bij de verwerking, ontwikkeling, opslag of het beheer van informatieactiva.

2.2 De reikwijdte omvat fysieke, digitale en in de cloud gehoste activa, waaronder gestructureerde en ongestructureerde gegevens, toepassingen, infrastructuur, netwerken en diensten.

2.3 Het beleid heeft betrekking op informatiebeveiligingsrisico's op strategisch, operationeel, project- en technisch niveau en is verplicht voor alle medewerkers, contractanten en dienstverleners die betrokken zijn bij ISMS-activiteiten.

2.4 Risicobeheer moet worden toegepast op de volgende scenario's:

2.4.1 implementatie van een nieuw project of systeem

2.4.1.1 significante wijzigingen (bijvoorbeeld in architectuur, eigenaarschap of processen)

2.4.1.2 onboarding van leveranciers en overeenkomsten met derden

2.4.1.3 incidentrespons en evaluatie na incidenten

2.4.1.4 periodieke organisatorische risicobeoordelingen of audits

3. Doelstellingen

3.1 Het vaststellen en operationaliseren van een herhaalbaar, organisatiebreed risicobeheerproces op basis van de methodologieën van ISO/IEC 27005 en ISO 31000.

3.2 Waarborgen dat risico's worden geïdentificeerd, geanalyseerd, geëvalueerd en behandeld met behulp van gestructureerde en herleidbare methoden, waaronder de toewijzing van risico-eigenaarschap en koppelingen met beheersmaatregelen.

3.3 Het onderhouden van een gecentraliseerd risicoregister en risicobehandelingsplan met versiebeheer, waarin de actuele risicostatus, dekking van beheersmaatregelen en voortgang van mitigerende maatregelen zijn vastgelegd.

3.4 Het afstemmen van risicobeslissingen op gedocumenteerde risicobereidheid en tolerantieniveaus, en het faciliteren van onderbouwde governancebesluiten over risicoacceptatie, mitigatie, overdracht of vermijding.

3.5 Het continu monitoren van risicotrends en waarborgen van de doeltreffendheid van risicobehandelingen, met ruimte voor proactieve bijsturing op basis van dreigingsontwikkelingen of wijzigingen in de bedrijfsvoering.

4. Rollen en verantwoordelijkheden

4.1 Topmanagement / Raad van Bestuur

4.1.1 Keurt het risicobeheerkader goed en stelt de aanvaardbare risicobereidheid en risicotolerantiedrempels vast.

4.1.2 Autoriseert risicobehandelingsstrategieën voor restrisico's die de tolerantie overschrijden.

4.1.3 Wijst middelen toe en houdt toezicht op een doeltreffende uitvoering van het risicobeheerprogramma.

4.2 ISMS-manager / Risicofunctionaris

4.2.1 Is eigenaar van dit beleid en bewaakt de afstemming ervan op de normen ISO/IEC 27001 en ISO/IEC 27005.

4.2.2 Geeft leiding aan het organisatiebrede risicobeoordelingsproces en onderhoudt het risicoregister en het risicobehandelingsplan.

4.2.3 Zorgt voor periodieke beoordelingen en escalatie van kernrisico-indicatoren naar het uitvoerend management of de ISMS-stuurgroep.

[... 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 Dit beleid en het bijbehorende raamwerk moeten jaarlijks worden beoordeeld, of:

9.1.1 na een groot risico-evenement of beveiligingsincident

9.1.2 na een significante organisatorische of technische wijziging

9.1.3 als reactie op auditbevindingen of nieuwe wettelijke of regelgevende vereisten

9.2 De ISMS-manager, risicofunctionaris en het complianceteam zijn gezamenlijk verantwoordelijk voor:

9.2.1 het initiëren van de beoordelingscyclus

9.2.2 het verzamelen van input van bedrijfseenheden

9.2.3 het herzien van procedures en drempels waar nodig

9.3 Alle herzieningen moeten:

9.3.1 onder versiebeheer vallen en worden geregistreerd

9.3.2 worden goedgekeurd door het topmanagement

9.3.3 worden gecommuniceerd aan belanghebbenden

9.3.4 gedurende minimaal 5 jaar worden bewaard in het auditarchief

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid hangt samen met de volgende informatiebeveiligingsbeleidslijnen:

10.1.1 P1 – Informatiebeveiligingsbeleid: stelt het overkoepelende model voor informatiebeveiligingsgovernance vast waarbinnen dit risicobeleid functioneert.

10.1.2 P2 – Beleid inzake governancerollen en -verantwoordelijkheden: definieert de verantwoordelijke eigenaren en governanceniveaus waarnaar in de risico-escalatiematrix wordt verwezen.

10.1.3 P5 – Wijzigingsbeheerbeleid: triggert herbeoordeling van risico's bij infrastructurele en organisatorische wijzigingen.

10.1.4 P13 – Beleid inzake gegevensclassificatie en etikettering: ondersteunt de impactbeoordeling tijdens risico-identificatie.

10.1.5 P33 – Beleid inzake audit- en nalevingsmonitoring: valideert de naleving van beleid, waaronder de volledigheid van het risicoregister en het bewijsmateriaal van behandelingen.

11. Referentienormen en -raamwerken

11.1 Dit beleid is expliciet afgestemd op de volgende normen en raamwerken om te waarborgen dat het voldoet aan internationale best practices en wettelijke en regelgevende verwachtingen voor het management van informatiebeveiligingsrisico's:

11.2 ISO/IEC 27001:

11.2.1 Clausule 6.1: stelt de vereisten vast voor het identificeren van risico's en kansen, waaronder de volledige levenscyclus van risicobeoordelingen en risicobehandelingen op het gebied van informatiebeveiliging. Dit beleid operationaliseert clausule 6.1.2 en 6.1.3 via een gestructureerd raamwerk dat gedocumenteerde risico-identificatie, analyse, evaluatie, behandeling en protocollen voor restrisicoacceptatie verplicht stelt.

11.2.2 Clausule 8.32: de integratie van risicogebaseerd denken in wijzigingsbeheerprocessen waarborgt dat alle significante organisatorische wijzigingen formele herbeoordelingen van risico's triggeren.

11.2.3 Clausule 10: continue verbetering is verankerd via regelmatige beleidsbeoordelingen, analyse van risicotrends en actualisaties van de SoA op basis van risico-inzichten.

11.3 ISO/IEC 27005:

11.3.1 Biedt gespecialiseerde en gedetailleerde richtlijnen voor het management van informatiebeveiligingsrisico's. Dit beleid implementeert het volledige procesmodel van ISO/IEC 27005 voor risico's: contextbepaling, risico-identificatie, risicoanalyse, risico-evaluatie, risicobehandeling, risicoacceptatie, risicocommunicatie, risicomonitoring en risicobeoordeling.

11.4 ISO 31000:

11.4.1 Dit beleid integreert de principes van ISO 31000, zoals betrokkenheid van leiderschap, integratie in besluitvorming en continue verbetering. Het waarborgt dat risicobeheer is verankerd in de cultuur en bedrijfsvoering van de organisatie.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Sluit aan op de NIST-richtlijn voor het uitvoeren van risicobeoordelingen, waaronder dreigingsidentificatie, kwetsbaarheidsanalyse, waarschijnlijkheidsinschatting en impactbepaling. De structuur van dit beleid weerspiegelt de door NIST gedefinieerde stappen voor risicobeoordeling en past deze toe op zowel technische als bedrijfsprocessen.

11.6 NIST SP 800-39:

11.6.1 Ondersteunt organisatiebrede risicogovernance, met nadruk op gelaagd risicobeheer op het niveau van de organisatie, missie-/bedrijfsprocessen en informatiesystemen. Dit beleid waarborgt dat risico-eigenaarschap op alle niveaus duidelijk is gedefinieerd en omvat behandelstrategieën op organisatieniveau.

11.7 AVG:

11.7.1 Artikel 24: vereist de implementatie van passende technische en organisatorische maatregelen om te waarborgen dat gegevensbeschermingsrisico's adequaat worden beheerd; dit wordt afgedekt via het gestructureerde risicoproces in dit beleid.

11.7.2 Artikel 25: gegevensbescherming door ontwerp en door standaardinstellingen sluit aan op het verankeren van risicobehandeling in systeem- en procesontwerpen.

11.7.3 Artikel 32: schrijft een risicogebaseerde benadering van beveiligingsmaatregelen voor; hieraan wordt voldaan via impactgebaseerde risicobeoordelingen en de selectie van beheersmaatregelen.

11.8 EU NIS2-richtlijn:

11.8.1 Artikel 21(2)(a–d): verplicht entiteiten om risicobeoordelingen uit te voeren, beleidslijnen voor risicoanalyse te implementeren en proportionele beveiligingsmaatregelen te waarborgen. Dit beleid voldoet aan deze verplichtingen via continue toepassing van de risicolevenscyclus en gedocumenteerde governance.

11.9 EU DORA:

11.9.1 Artikel 5: verplicht een gedocumenteerd ICT-risicobeheerkader; dit wordt volledig afgedekt door de architectuur van dit beleid, inclusief SoA-mapping en KRI's.

11.9.2 Artikel 6: vereist integratie van risicobeheer in strategieën voor operationele weerbaarheid, wat wordt geborgd via escalatiematrices en het volgen van kritieke activa.

11.10 COBIT 2019:

11.10.1 APO12 – Manage Risk: sluit direct aan op de invoering door de organisatie van een gestructureerde benadering van risicobeheer, met toewijzing van rollen, opvolging van behandelingen en borging van verantwoordingsplicht op bestuursniveau.

11.10.2 MEA01 – Monitoren, evalueren en beoordelen van prestaties en conformiteit: weerspiegeld in de focus van dit beleid op trendanalyse, monitoring van KRI's en integratie van auditfeedback in cycli van continue verbetering.