					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P27					Documenttitel: **Beleid inzake het gebruik van cloudservices**							
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 8	Vereisten voor operationele planning en beheersing van cloudomgevingen.
ISO/IEC 27002:2022	Beheersmaatregelen 5.23–5.25	Vereisten inzake het gebruik, beleid en de beveiliging van cloudservices.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12–SC-28, SR-5	Gebruik van externe systemen, contractuele en technische vereisten, cryptografische bescherming en beveiliging van de toeleveringsketen.
AVG	Artikelen 28, 32, Hoofdstuk V	Vereisten voor cloudverwerkers, beveiliging van de verwerking en gegevensdoorgiften.
EU NIS2	Artikel 21(2)(f, i)	Vereisten inzake derdenrisico en de toeleveringsketen.
EU DORA	Artikelen 5(2), 28	Toezicht op ICT en derde partijen (cloud) voor financiële entiteiten.
COBIT 2019	BAI04, DSS01, DSS05	Beschikbaarheid van cloudservices, operationeel beheer en beveiligingsbeheer.

1. Doel

1.1 Dit beleid stelt de verplichte vereisten van de organisatie vast voor het veilige, conforme en verantwoorde gebruik van cloudservices binnen de servicemodellen Infrastructure as a Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS).

1.2 Dit beleid heeft tot doel te waarborgen dat cloudservices worden ingevoerd en beheerst op een wijze die de vertrouwelijkheid, integriteit en beschikbaarheid van informatieactiva beschermt en tegelijkertijd voldoet aan wettelijke, reglementaire en contractuele verplichtingen.

1.3 Het beleid definieert beheersmaatregelen om cloudrisico's te beheersen, gegevens te beschermen, naleving door aanbieders te monitoren en ongeautoriseerd gebruik te voorkomen. Daarnaast ondersteunt het zakelijke innovatie via cloudplatforms door informatiebeveiliging, operationele betrouwbaarheid en kostenefficiëntie op elkaar af te stemmen.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle medewerkers, contractanten, externe dienstverleners en externe consultants die namens de organisatie cloudservices toewijzen, configureren, benaderen, beheren of gebruiken.

2.2 Het is van toepassing op alle omgevingen waarin gegevens of workloads van de organisatie worden verwerkt, waaronder:

2.2.1 publieke, private, hybride en communitycloud-implementaties

2.2.2 alle cloudservicemodellen (IaaS, PaaS, SaaS)

2.2.3 multicloud- en federatieve architecturen

2.2.4 gebruik van shadow-IT of persoonlijke cloudaccounts voor bedrijfsdoeleinden

2.3 Dit beleid omvat alle gegevensclassificaties en is van toepassing op zowel interne systemen als door leveranciers gehoste platforms waarop gegevens in eigendom van de organisatie of gereguleerde gegevens worden opgeslagen of verwerkt.

3. Doelstellingen

3.1 Het waarborgen van veilig en consistent gebruik van cloudtechnologieën door middel van duidelijk vastgelegde gebruiksrichtlijnen, beveiligingsbaselines en governancerollen.

3.2 Het minimaliseren van operationele en reglementaire risico's die samenhangen met cloudcomputing, waaronder ongeautoriseerde toegang, datalekken, foutieve configuraties, niet-naleving en verstoring van de dienstverlening.

3.3 Het afdwingen van beveiligings- en privacyvereisten voor alle cloudleveranciers en het verifiëren van naleving via contractuele bepalingen, beoordelingen en auditrechten.

3.4 Het mogelijk maken van schaalbare en veerkrachtige invoering van cloudservices zonder afbreuk te doen aan de risicohouding op het gebied van informatiebeveiliging, wettelijke vereisten of bedrijfscontinuïteit.

3.5 Het afstemmen van cloudgovernance en cloudgebruik op het ISMS van de organisatie, wettelijke verplichtingen (bijvoorbeeld AVG, DORA), sectorspecifieke richtsnoeren en in de sector erkende best practices (bijvoorbeeld NIST, COBIT).

4. Rollen en verantwoordelijkheden

4.1 Directie

4.1.1 Keurt het beleid inzake het gebruik van cloudservices en de strategische roadmap voor cloudadoptie goed.

4.1.2 Beoordeelt en bekrachtigt uitzonderingen met een hoog risico op de standaardgovernancevereisten voor cloudgebruik.

4.1.3 Zorgt ervoor dat cloudinitiatieven beschikken over toereikende financiering, toezicht en integratie met kaders voor enterprise risk management.

4.2 Chief Information Security Officer (CISO)

4.2.1 Is eigenaar van dit beleid en van het organisatiebrede register van cloudservices.

4.2.2 Keurt de onboarding van nieuwe cloudproviders goed op basis van due diligence en risicobeoordeling.

4.2.3 Beoordeelt nalevingsdocumentatie van aanbieders en valideert de afstemming op beveiligingsvereisten.

[... 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 moet ten minste jaarlijks worden beoordeeld en waar nodig worden bijgewerkt om blijvende afstemming te waarborgen met:

9.1.1 evoluerende wettelijke en reglementaire vereisten (bijvoorbeeld AVG, NIS2, DORA)

9.1.2 wijzigingen in de normen ISO/IEC 27001 of ISO/IEC 27002

9.1.3 actualisaties van de cloudarchitectuur, het dreigingslandschap of het serviceportfolio van de organisatie

9.1.4 incidentonderzoeken, auditbevindingen of geleerde lessen uit operationeel gebruik

9.2 De CISO is verantwoordelijk voor het initiëren van de beoordeling en het bijeenroepen van relevante stakeholders, waaronder:

9.2.1 cloudbeveiligingsarchitect

9.2.2 juridisch en complianceteam

9.2.3 inkoop- en leveranciersmanagers

9.2.4 service-eigenaren en IT-operatie

9.3 Alle actualisaties moeten:

9.3.1 onder versiebeheer staan en van een datum zijn voorzien

9.3.2 worden goedgekeurd door de directie

9.3.3 worden gecommuniceerd aan betrokken partijen, waaronder medewerkers, contractanten en derde partijen

9.3.4 worden gearchiveerd overeenkomstig het interne documentatiebeleid

9.4 Tussentijdse beoordelingen kunnen worden getriggerd door:

9.4.1 nieuwe verbintenissen met CSP's of majeure migraties

9.4.2 opkomende dreigingen voor cloudinfrastructuur

9.4.3 materiële wijzigingen in contractuele, wettelijke of sectorspecifieke verplichtingen

10. Gerelateerde beleidsdocumenten en samenhang

10.1 Dit beleid hangt nauw samen met en is afhankelijk van de volgende interne beleidsdocumenten:

10.1.1 P1 – Informatiebeveiligingsbeleid: stelt de overkoepelende beginselen vast voor de veilige werking van systemen en diensten, die dit beleid afdwingt binnen de cloudcontext.

10.1.2 P5 – Wijzigingsbeheerbeleid: alle wijzigingen in cloudconfiguraties moeten de procedures voor wijzigingsbeheer volgen zoals vastgelegd in P5.

10.1.3 P13 – Beleid inzake gegevensclassificatie en etikettering: bepaalt hoe gegevens worden beoordeeld vóór overdracht naar de cloud en hoe beheersmaatregelen zoals encryptie en gegevensresidentie worden toegepast.

10.1.4 P18 – Beleid inzake cryptografische beheersmaatregelen: bevat standaarden voor encryptie, sleutelbeheer en het gebruik van cryptografische algoritmen, die rechtstreeks worden toegepast in configuraties van cloudservices.

10.1.5 P22 – Logging- en monitoringbeleid: specificeert vereisten voor het verzamelen, bewaren en analyseren van logbestanden die in cloudomgevingen moeten worden afgedwongen.

10.1.6 P30 – Incidentresponsbeleid: definieert procedures voor escalatie, indamming en remediatie van cloudgerelateerde beveiligingsincidenten.

10.1.7 P33 – Beleid inzake audit- en nalevingsmonitoring: ondersteunt auditgereedheid en voortdurende assurance dat cloudbeheersmaatregelen worden afgedwongen en gemonitord.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001: Clausule 8.1 – Operationele planning en beheersing: vereist dat organisaties processen implementeren en beheersen die nodig zijn om aan informatiebeveiligingsvereisten te voldoen, inclusief processen waarbij cloudomgevingen betrokken zijn.

11.2 ISO/IEC 27002:2022 – Beheersmaatregelen 5.23 tot en met 5.25:

11.2.1 Bijlage A Beheersmaatregel 5.23 – Gebruik van cloudservices: vereist een risicogebaseerde beoordeling, formele autorisatie en documentatie van het gebruik van cloudservices.

11.2.2 Bijlage A Beheersmaatregel 5.24 – Beleid inzake het gebruik van cloudservices: vereist het vaststellen en handhaven van formeel beleid voor cloudgebruik dat is afgestemd op de behoeften en risico's van de organisatie.

11.2.3 Bijlage A Beheersmaatregel 5.25 – Beveiliging in cloudservices: vereist integratie van beveiliging, contractuele waarborgen en monitoring van cloudgehoste workloads en gegevens.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Gebruik van externe systemen: vereist vastgelegde regels en voorwaarden voor toegang tot middelen van de organisatie vanuit externe of cloudgebaseerde systemen.

11.3.2 SA-9(5) – Externe informatiedienstsystemen: vereist contractuele beveiligingsvereisten, toezicht en continue monitoring voor cloudsystemen van derde partijen.

11.3.3 SC-12 tot en met SC-28 – Cryptografische bescherming, grensbeveiliging en transmissie-integriteit: sluiten aan op de vereisten inzake encryptie, identiteit en toegang voor cloudgehoste diensten en gegevens in transit.

11.3.4 SR-5 – Bescherming van de toeleveringsketen: ondersteunt beoordeling en contractuele beheersing van CSP's die bij de dienstverlening betrokken zijn.

11.4 AVG (2016/679):

11.4.1 Artikel 28 – Verplichtingen van de verwerker: vereist formele contracten met cloudproviders om de beveiliging, vertrouwelijkheid en controleerbaarheid van de verwerking van persoonsgegevens te waarborgen.

11.4.2 Artikel 32 – Beveiliging van de verwerking: ondersteunt de toepassing van encryptie, toegangscontrole, logging en andere waarborgen in cloudomgevingen.

11.4.3 Hoofdstuk V – Internationale gegevensdoorgiften: vereist rechtmatige doorgifte van gegevens buiten de EU/EER met gebruikmaking van waarborgen zoals SCC's of adequaatheidsbesluiten.

11.5 EU NIS2-richtlijn (2022/2555):

11.5.1 Artikel 21(2)(f, i): vereist dat entiteiten risico's van cloudserviceproviders van derde partijen beheren en de integriteit van de digitale toeleveringsketen waarborgen via contractuele en technische maatregelen.

11.6 EU DORA (2022/2554):

11.6.1 Artikel 5(2) – Governance van ICT-risico's: vereist integratie van ICT-risico's van derde partijen, waaronder cloudservices, in de algehele risicogovernance.

11.6.2 Artikel 28 – Toezicht op kritieke ICT-dienstverleners van derde partijen: vereist dat financiële entiteiten afhankelijkheden van cloudproviders, hun risicohouding op het gebied van informatiebeveiliging en hun weerbaarheid monitoren, beheersen en rapporteren.

11.7 COBIT 2019:

11.7.1 BAI04 – Beschikbaarheid en capaciteit beheren: waarborgt dat cloudservices veerkrachtig zijn, worden gemonitord en voldoen aan vastgestelde prestatiecriteria.

11.7.2 DSS01 – Operaties beheren: ondersteunt operationele integratie, incidentafhandeling en baselineconfiguraties voor cloudgehoste platforms.

11.7.3 DSS05 – Beveiligingsdiensten beheren: stuurt op implementatie van cloudspecifieke beveiligingsmaatregelen, monitoring en incidentpreventie binnen digitale diensten.