					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P13					Documenttitel: **Beleid inzake gegevensclassificatie en etikettering**							
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**

1. Doel

1.1 Dit beleid definieert het formele kader voor de classificatie en etikettering van de informatieactiva van de organisatie op basis van gevoeligheid, risicoblootstelling en nalevingsverplichtingen.

1.2 Het waarborgt dat alle informatie — ongeacht of deze wordt opgeslagen, verzonden of verwerkt — duidelijk wordt geclassificeerd en geëtiketteerd op een wijze die het vereiste beschermings- en verwerkingsniveau kenbaar maakt.

1.3 Dit beleid schrijft een gestructureerd classificatiemodel voor dat is afgestemd op het informatiebeveiligingsrisicomanagement van de organisatie en de doelstellingen voor vertrouwelijkheid, integriteit en beschikbaarheid (CIA) ondersteunt voor zowel digitale als fysieke gegevensdragers.

1.4 Deze beheersmaatregel is essentieel voor het faciliteren van rolgebaseerde toegang, auditgereedheid, passende gegevensuitwisseling en de doeltreffende inzet van technische beheersmaatregelen zoals encryptie, back-up en monitoring.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 Alle informatieactiva van de organisatie, met inbegrip van documenten, databases, registraties en communicatie

2.1.2 Alle gegevensvormen, waaronder digitaal, geprint, schriftelijk en mondeling

2.1.3 Alle omgevingen: on-premises, op afstand, mobiel en in de cloud

2.1.4 Alle medewerkers, contractanten, dienstverleners en externe verwerkers die informatie van de organisatie creëren, verwerken of opslaan

2.2 De reikwijdte omvat intern ontwikkelde inhoud, extern verkregen gegevens, persoonsgegevens die onder verplichtingen uit privacywetgeving vallen (bijv. AVG), en informatie die wordt uitgewisseld met klanten, partners en toezichthouders.

2.3 Het beleid is van toepassing op alle systemen die worden gebruikt om gegevens op te slaan of te verzenden, waaronder bedrijfstoepassingen, bestandsservers, e-mailsystemen, cloudplatforms en back-upopslagplaatsen.

3. Doelstellingen

3.1 Het vaststellen van een gestandaardiseerd, organisatiebreed classificatieschema op basis van de impact van blootstelling of compromittering van gegevens.

3.2 Waarborgen dat alle informatie zichtbaar en blijvend wordt geëtiketteerd, zodat het classificatieniveau en de vereisten voor verwerking duidelijk zijn.

3.3 Het afdwingen van beheersmaatregelen voor gegevensverwerking en toegangsbeveiliging die zijn afgestemd op de classificatie, waaronder encryptie, logging, transportbeveiliging en bewaartermijnen.

3.4 Het ondersteunen van naleving van internationale normen (ISO/IEC 27001, 27002), wettelijke kaders (AVG, NIS2, DORA) en intern beleid inzake risicomanagement.

3.5 Waarborgen dat alle gebruikers hun verantwoordelijkheden begrijpen voor het beschermen van gegevens, het toepassen van etiketten en het correct verwerken van geclassificeerde gegevens.

3.6 Het borgen van traceerbaarheid tussen classificatiestatus, bijbehorende beheersmaatregelen en de bedrijfsmiddeleninventaris van de organisatie ten behoeve van audit en naleving.

4. Rollen en verantwoordelijkheden

4.1 Chief Information Security Officer (CISO)

4.1.1 Is eigenaar van het beleid inzake gegevensclassificatie en etikettering en ziet toe op afstemming met wettelijke, contractuele en operationele vereisten.

4.1.2 Keurt classificatieniveaus, etiketteringsstandaarden en beleidsherzieningen goed.

4.1.3 Houdt toezicht op de naleving van het beleid via audits, meetwaarden en beoordelingen van uitzonderingen.

4.1.4 Coördineert de interdisciplinaire governance met Juridische Zaken, Compliance, privacy- en risicoteams.

4.2 Eigenaren van informatieactiva

4.2.1 Zijn verantwoordelijk voor het classificeren van informatieactiva onder hun beheer met gebruikmaking van het classificatieschema van de organisatie.

4.2.2 Passen classificatie-etiketten toe op het moment van creatie, wijziging of ontvangst.

4.2.3 Beoordelen periodiek de classificatie van bedrijfsmiddelen, met name naar aanleiding van wijzigingen in gevoeligheid, wettelijke reikwijdte of bedrijfswaarde.

4.2.4 Zien erop toe dat gevoelige gegevens gedurende de gehele levenscyclus passend worden verwerkt en geëtiketteerd.

[... 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 Dit beleid moet ten minste jaarlijks worden beoordeeld om afstemming te waarborgen met:

9.1.1 Ontwikkelingen in wet- en regelgeving (bijv. AVG, NIS2, DORA)

9.1.2 Actualisaties van ISO/IEC 27001- of 27002-richtlijnen voor classificatie

9.1.3 Organisatorische wijzigingen die van invloed zijn op de gevoeligheid van gegevens of het eigenaarschap

9.1.4 Technologische wijzigingen, waaronder nieuwe platforms voor document- of gegevensbeheer

9.2 De Chief Information Security Officer (CISO) moet de beoordeling initiëren in samenwerking met de Informatiebeveiligingscommissie, Juridische Zaken en betrokken bedrijfseenheden.

9.3 Beoordelingen moeten het volgende omvatten:

9.3.1 De doeltreffendheid van classificatieafdwinging en de naleving door gebruikers

9.3.2 Analyse van incidenten of uitzonderingen die verband houden met onjuiste classificatie

9.3.3 Gebruikersfeedback over etiketteringstools of richtsnoeren

9.3.4 Benchmarking ten opzichte van classificatiestandaarden in de sector

9.4 Beleidsactualisaties moeten onder versiebeheer staan, worden gedocumenteerd in de ISMS-repository en worden gecommuniceerd aan al het relevante personeel, met nadruk op nieuwe verantwoordelijkheden of wijzigingen in tooling.

9.5 Nieuwe medewerkers moeten tijdens onboarding kennisnemen van de actuele versie van dit beleid. Alle medewerkers moeten een opfristraining volgen na significante beleidswijzigingen.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid wordt rechtstreeks ondersteund door en geeft uitvoering aan beheersmaatregelen die zijn beschreven in de volgende gerelateerde beleidslijnen:

10.1.1 P4 - Beleid inzake toegangsbeveiliging: Toegang tot informatie wordt bepaald door classificatieniveaus; voor gevoeliger gegevens is strengere toegangsbeveiliging en autorisatie vereist.

10.1.2 P11 - Beleid inzake beheer van gebruikersaccounts en privileges: Versterkt de toewijzing van privileges op basis van het need-to-know-principe, dat wordt bepaald door classificatieniveaus.

10.1.3 P12 - Beleid inzake assetmanagement: Waarborgt dat elk bedrijfsmiddel in de inventaris de bijbehorende classificatie en het bijbehorende etiket bevat, ter ondersteuning van traceerbaarheid en verantwoordingsplicht.

10.1.4 P14 - Beleid inzake gegevensbewaring en afvoer: Regels voor bewaring en afvoer worden bepaald door het classificatieniveau van gegevens en wettelijke bewaarplichten.

10.1.5 P18 - Beleid inzake cryptografische beheersmaatregelen: Past passende encryptiestandaarden toe op basis van de classificatie van het informatieactief.

10.1.6 P22 - Beleid inzake logging en monitoring: Maakt toezicht op toegang tot en verplaatsing van geclassificeerde informatie mogelijk en waarborgt auditbaarheid en detectie van onjuiste etikettering of misbruik.

10.2 Elke samenhang zorgt voor consistente bescherming van informatie gedurende de volledige levenscyclus, van creatie en classificatie tot veilige verwerking, opslag, verzending en uiteindelijke vernietiging.

11. Referentienormen en -raamwerken

11.1 Dit beleid is afgestemd op internationaal erkende normen en regelgevende kaders voor de classificatie en etikettering van gevoelige informatie.

11.2 ISO/IEC 27001

11.2.1 Clausule 4.2 - Inzicht in de behoeften en verwachtingen van belanghebbende partijen. Classificatievereisten vloeien vaak voort uit wettelijke, regelgevende of contractuele verplichtingen die door belanghebbende partijen worden opgelegd (bijv. AVG, geheimhoudingsovereenkomsten met klanten) en moeten in dit beleid worden weerspiegeld.

11.2.2 Clausule 6.1.3 - Informatiebeveiligingsrisicobehandeling. Classificatie heeft direct invloed op de selectie van beheersmaatregelen voor risicobehandeling, waaronder toegangsbeveiliging, encryptie en bewaring, op basis van de gevoeligheid van gegevens.

11.2.3 Clausule 7.2 - Competentie. Dit beleid schrijft voor dat personeel dat verantwoordelijk is voor classificatie en etikettering passend moet zijn opgeleid; dit valt onder de competentievereisten.

11.2.4 Clausule 7.3 - Bewustzijn. Dit beleid vereist dat alle gebruikers op de hoogte zijn van classificatieniveaus en hun verantwoordelijkheden bij de verwerking van informatie, in lijn met de verplichtingen inzake bewustwording.

11.2.5 Clausule 7.5 - Gedocumenteerde informatie. Het classificatiebeleid zelf is een beheerst document en de procedures, opleidingsregistraties en classificatie-etiketten maken deel uit van de gedocumenteerde informatie.

11.2.6 Clausule 8.1 - Operationele planning en beheersing. Classificatie en etikettering zijn operationele processen die zijn ingebed in het beheer van de gegevenslevenscyclus, en deze clausule waarborgt dat dergelijke activiteiten worden gepland, geïmplementeerd en beheerst.

11.2.7 Clausule 9.1 - Monitoring, meting, analyse en evaluatie. Dit beleid bevat bepalingen voor het monitoren van classificatienaleving, incidenttrends en de doeltreffendheid van het etiketteringsschema.

11.2.8 Clausule 10.1 - Non-conformiteit en corrigerende maatregel. Dit beleid definieert reacties op onjuiste classificatie, waaronder corrigerende maatregelen zoals hertraining, actualisaties en uitzonderingsbeheer.

11.3 ISO/IEC 27002:2022

11.3.1 Beheersmaatregel 5.12 - Classificatie van informatie. Deze beheersmaatregel waarborgt dat informatie wordt geclassificeerd op basis van gevoeligheid, waarde en kriticiteit — precies wat dit beleid formaliseert.

11.3.2 Beheersmaatregel 5.13 - Etikettering van informatie. Deze beheersmaatregel vereist passende etikettering van informatie in overeenstemming met het classificatieniveau; dit wordt volledig in dit beleid behandeld.

11.3.3 Beheersmaatregel 5.10 - Aanvaardbaar gebruik van informatie en andere gerelateerde activa. Dit beleid schrijft voor hoe gebruikers geclassificeerde gegevens moeten verwerken en ondersteunt daarmee direct het aanvaardbaar gebruik en het voorkomen van misbruik.

11.3.4 Beheersmaatregel 5.11 - Teruggave van activa. Classificatie helpt waarborgen dat gevoelige gegevens worden geïdentificeerd en veilig worden teruggegeven of geschoond wanneer een medewerker of leverancier uit dienst treedt.

11.3.5 Beheersmaatregel 5.9 - Inventaris van informatie en andere gerelateerde activa. Classificatie is vaak gekoppeld aan de bedrijfsmiddeleninventaris, waarin het classificatieniveau van elk item moet zijn opgenomen om passende toewijzing van beheersmaatregelen te ondersteunen.

11.3.6 Beheersmaatregel 5.14 - Overdracht van informatie. Classificatieniveaus beïnvloeden beheersmaatregelen voor interne en externe gegevensoverdracht (bijv. encryptie, goedkeuring, toegangsbeperkingen).

11.3.7 Beheersmaatregel 8.12 - Preventie van gegevenslekken. Het afdwingen van classificatie en etikettering ondersteunt het voorkomen van ongeautoriseerde openbaarmaking en gegevensverlies.

11.3.8 Beheersmaatregel 8.11 - Gegevensmaskering. Bepaalde classificatieniveaus (bijv. Vertrouwelijk, Beperkt) kunnen maskering verplicht stellen wanneer gegevens worden gebruikt in test-, ontwikkel- of analyseomgevingen.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Beleid en procedures voor systeem- en communicatiebeveiliging: ondersteunt classificatiebeleid als onderdeel van overkoepelende gegevensbescherming.

11.4.2 AC-16 - Beveiligingsattributen: implementeert toegangsafdwinging op basis van classificatiemetadata en gebruikersrechten.

11.4.3 MP-3 / MP-5 - Markering van media en transportbeveiliging: dwingt etikettering en bescherming van gegevens in rust en tijdens transport af op basis van classificatie.

11.5 AVG (2016/679)

11.5.1 Artikel 5 - Beginselen inzake gegevensbescherming: vereist dat persoonsgegevens veilig en proportioneel ten opzichte van hun gevoeligheid worden verwerkt.

11.5.2 Artikel 32 - Beveiliging van de verwerking: bevestigt classificatie als mechanisme voor risicogebaseerde gegevensbescherming en passende technische maatregelen.

11.6 EU NIS2-richtlijn (2022/2555)

11.6.1 Artikel 21(2)(a): vereist beleid voor informatiebeveiligingsrisicomanagement, waaronder beheersmaatregelen voor classificatie van activa en gegevens.

11.6.2 Artikel 21(3): stimuleert de invoering van maatregelen om passende gegevensverwerking af te dwingen — ondersteund door classificatiegebaseerde etikettering.

11.7 EU DORA (2022/2554)

11.7.1 Artikel 5 - Governance en beheersing: vereist governancestructuren waarin gegevensactiva worden geclassificeerd voor de beheersing van ICT-risico's.

11.7.2 Artikel 9 - ICT-risicobeheer: legt technische en organisatorische maatregelen op voor kritieke ICT-activa, waaronder classificatie en etikettering.

11.8 COBIT 2019

11.8.1 DSS05.02 - Beheer van beveiligingsdiensten: dwingt informatiebeveiligingsclassificaties af om bescherming van gegevens binnen de organisatie te waarborgen.

11.8.2 MEA03 - Monitoren, evalueren en assesseren van naleving: ondersteunt periodieke audit en beoordeling van classificatiepraktijken om beleidsnaleving en volwassenheid te waarborgen.