| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Voer hier de naam van de geregistreerde rechtspersoon in | | | | | | | |
| Documentnummer:<br>P13S | | | | | Documenttitel:<br>**Beleid inzake gegevensclassificatie en etikettering** | | | | | | | |
| Versie:<br>1.0 | | Ingangsdatum:<br>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 5.3, 8 | |
| ISO/IEC 27002:2022 | Beheersmaatregelen 5.12, 5.13 | |
| NIST SP 800-53 Rev.5 | AC-16, MP-3, MP-5 | |
| EU NIS2 | Artikel 21(2)(a) | |
| EU DORA | Artikel 5(8) | |
| COBIT 2019 | BAI03.05, DSS05 | |
| AVG | Artikelen 5, 32 | |

**1. Doel**

1.1 Dit beleid bepaalt hoe alle informatie die door de organisatie wordt verwerkt, moet worden geclassificeerd en gelabeld om te waarborgen dat de vertrouwelijkheid, integriteit en beschikbaarheid gedurende de volledige levenscyclus behouden blijven.

1.2 Dit beleid maakt consistente gegevensverwerking mogelijk door aan informatie passende beschermingsniveaus toe te kennen op basis van gevoeligheid, bedrijfsimpact of wettelijke verplichtingen.

1.3 Gegevensclassificatie en labeling helpen het risico op onbedoelde openbaarmaking, ongeautoriseerde toegang of onjuiste verwerking van gevoelige gegevens te beperken, in het bijzonder binnen het mkb, waar vaak eenvoudigere systemen en minder geformaliseerde beheersmaatregelen worden toegepast.

1.4 Dit beleid is van essentieel belang voor ISO/IEC 27001-certificering en naleving van wet- en regelgeving, in het bijzonder gegevensbeschermingswetgeving zoals de AVG en cyberbeveiligingskaders zoals NIS2 en DORA.

**2. Reikwijdte**

**2.1 Dit beleid is van toepassing op alle gegevens van de organisatie, ongeacht formaat of locatie, waaronder:**

2.1.1 Elektronische documenten, spreadsheets, e-mails, formulieren, afbeeldingen en gescande bestanden

2.1.2 Fysieke documenten, zoals afgedrukte registraties, rapporten, facturen en notities

2.1.3 Gegevens die worden opgeslagen of verwerkt in clouddiensten, op lokale servers, verwisselbare media of persoonlijke apparaten die voor zakelijke doeleinden worden gebruikt

2.1.4 Tijdelijke of vluchtige gegevens die tijdens de bedrijfsvoering worden gegenereerd, zoals logbestanden, cachebestanden en e-mails

2.2 Alle medewerkers, opdrachtnemers, tijdelijke krachten en externe dienstverleners met toegang tot gegevens van de organisatie moeten dit beleid naleven.

2.3 Dit beleid geldt gedurende de volledige gegevenslevenscyclus: vanaf creatie en opslag, via toegang en overdracht, tot archivering of verwijdering.

**3. Doelstellingen**

3.1 Een eenvoudig en afdwingbaar classificatiemodel vaststellen dat binnen de gehele organisatie gemakkelijk kan worden begrepen en toegepast.

3.2 Vereisen dat elk gegevensobject wordt geclassificeerd op basis van gevoeligheid en dienovereenkomstig wordt gelabeld om juiste verwerking, opslag en toegang te sturen.

3.3 Waarborgen dat labeling van gegevens wordt geïntegreerd in bedrijfsprocessen zoals indiensttreding, projectinitiatie en systeemconfiguratie.

3.4 Het risico op een datalek beperken door beveiligingsmaatregelen, zoals versleuteling en toegangsbeperking, toe te passen overeenkomstig het classificatieniveau.

3.5 Naleving van privacywetgeving en wetgeving inzake informatiebeveiliging waarborgen door aantoonbaar te maken dat gevoelige gegevens, zoals persoonsgegevens, financiële gegevens of bedrijfsvertrouwelijke informatie, correct zijn gelabeld en beheerd.

3.6 Verantwoordelijkheid voor classificatiebesluiten vastleggen en periodieke herzieningen en actualisaties waarborgen op basis van veranderende zakelijke en juridische behoeften.

## 4. Rollen en verantwoordelijkheden

### 4.1 Algemeen directeur (GM)

4.1.1 Is eigenaar van dit beleid en keurt het classificatiemodel goed.

4.1.2 Houdt toezicht om te waarborgen dat classificatieverantwoordelijkheden worden gedelegeerd en nageleefd.

4.1.3 Moet uitzonderingen op classificatie- of labelvereisten beoordelen en autoriseren.

4.1.4 Waarborgt dat gegevensverwerking voldoet aan complianceverplichtingen op grond van wetgeving zoals de AVG en DORA.

### 4.2 Informatie-eigenaar / gegevensbeheerder

4.2.1 Kent bij creatie of verwerving een initiële classificatie toe aan elke nieuwe gegevensverzameling of elk informatiebedrijfsmiddel.

4.2.2 Zorgt ervoor dat zichtbare labels, zoals documentkoppen, voetteksten, watermerken en mapnamen, waar van toepassing worden aangebracht.

4.2.3 Beoordeelt classificaties periodiek om relevantie, juistheid en noodzakelijke wijzigingen te verifiëren, bijvoorbeeld na declassificatie of publicatie.

4.2.4 Werkt samen met de IT-verantwoordelijke om technische bescherming op basis van classificatie af te dwingen, zoals toegangsrechten en versleuteling.

[ ... 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 actualisatie

### 9.1 Dit beleid moet jaarlijks door de GM en de gegevensbeheerder worden herzien om te waarborgen dat het aansluit op:

9.1.1 Wijzigingen in de bedrijfsvoering of gegevenstypen

9.1.2 Nieuwe regelgevende vereisten, bijvoorbeeld op het gebied van gegevensbescherming of financieel toezicht

9.1.3 Technologische veranderingen die van invloed zijn op mogelijkheden voor labeling of classificatie

9.2 De herziening moet actualisaties omvatten van classificatiecategorieën, labelingtools of -praktijken en inhoud voor bewustwording en training.

9.3 Beleidsherzieningen moeten door de GM worden goedgekeurd en aan alle medewerkers worden gecommuniceerd. Een registratie van versiewijzigingen moet voor auditdoeleinden worden bewaard.

## 10. Gerelateerde beleidsdocumenten en samenhang

10.1 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: wijst verantwoordelijkheid toe voor beleidseigenaarschap en handhaving.

10.2 P4S – Beleid inzake toegangscontrole: stemt systeemtoegang af op classificatieniveaus van gegevens.

10.3 P12S – Beleid inzake assetmanagement: borgt de registratie van fysieke en digitale bedrijfsmiddelen waarin geclassificeerde gegevens worden opgeslagen.

10.4 P17S – Beleid inzake gegevensbescherming en privacy: regelt de bescherming van persoonsgegevens, waarvan een groot deel als Vertrouwelijk is geclassificeerd.

10.5 P30S – Incidentresponsbeleid: definieert escalatieroutes en responsprocedures bij classificatieovertredingen of blootstelling van gegevens.

## 11. Referentienormen en -raamwerken

### 11.1 ISO/IEC 27001

11.1.1 Clausule 5.3: vereist duidelijk vastgelegde verantwoordelijkheden voor gegevensverwerking en bescherming.

11.1.2 Clausule 8.1: schrijft operationele planning en beheersmaatregelen voor, waaronder maatregelen die samenhangen met gegevensclassificatie.

### 11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 5.12: geeft richtlijnen voor informatieclassificatie op basis van risico's en regelgevende vereisten.

11.2.2 Beheersmaatregel 5.13: beschrijft praktische labelmechanismen en bijbehorende verwerkingsregels.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: vereist markering van informatie zodat beschermingsmaatregelen aansluiten op de classificatie.

11.3.2 MP-3 / MP-5: geven richtlijnen voor het labelen en beheersen van media en uitvoer.

### 11.4 AVG

11.4.1 Artikelen 5 en 32: verplichten gegevensminimalisatie en integriteit door passende classificatie en verwerkingsmaatregelen.

### 11.5 EU NIS2

11.5.1 Artikel 21(2)(a): schrijft technische en organisatorische beheersmaatregelen voor ten behoeve van risicogebaseerde gegevensbescherming.

### 11.6 EU DORA

11.6.1 Artikel 5(8): vereist dat organisaties gegevensactiva classificeren als onderdeel van hun ICT-risicobeheerprogramma.

### 11.7 COBIT 2019

11.7.1 BAI03.05: verlangt informatieclassificatie en op risico afgestemde bescherming.

11.7.2 DSS05.02: behandelt de handhaving van classificatiegebaseerde beheersmaatregelen en de monitoring daarvan.