					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P12					Documenttitel: **Beleid inzake beheer van bedrijfsmiddelen**							
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 stelt de verplichte organisatorische vereisten vast voor het identificeren, classificeren, beheren en beveiligen van informatieactiva gedurende hun volledige levenscyclus. Het ondersteunt organisatiebrede governance van hardware, software, gegevens, cloudactiva en immateriële informatieactiva, met inbegrip van mobiele, externe en door derden beheerde omgevingen.

1.2 Het doel van dit beleid is volledige zichtbaarheid op het informatieactivalandschap van de organisatie te waarborgen, zodat doeltreffende beheersmaatregelen, toewijzing van eigenaarschap, afstemming op nalevingsverplichtingen en verantwoorde buitengebruikstelling of afvoer mogelijk zijn.

1.3 Dit beleid is afgestemd op ISO/IEC 27001:2022 Annex A.5.9 door het verplicht stellen van het bijhouden van een gecentraliseerde inventaris van informatie en bijbehorende activa. Het waarborgt accountability door elk bedrijfsmiddel te koppelen aan een eigenaar en classificatiegedreven bescherming toe te passen op basis van bedrijfssensitiviteit en wettelijke vereisten.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle werknemers, contractanten, externe leveranciers en dienstverleners die informatieactiva beheren, gebruiken, raadplegen, opslaan of verwerken die eigendom zijn van of onder zeggenschap staan van de organisatie.

2.2 De reikwijdte omvat alle categorieën bedrijfsmiddelen, waaronder:

2.2.1 fysieke bedrijfsmiddelen: laptops, desktops, mobiele apparaten, verwijderbare media, printers, netwerkapparatuur

2.2.2 digitale bedrijfsmiddelen: software, toepassingen, systeemimages, databases, back-upgegevens, encryptiesleutels

2.2.3 informatieactiva: gestructureerde en ongestructureerde gegevens, rapporten, e-mails, intellectueel eigendom

2.2.4 cloud- en virtuele bedrijfsmiddelen: IaaS-, SaaS- en PaaS-omgevingen, virtuele machines, containers

2.2.5 logische bedrijfsmiddelen: domeinnamen, licenties, gebruikersaccounts, baselineconfiguraties

2.3 Dit beleid is eveneens van toepassing op bedrijfsmiddelen die worden gebruikt in regelingen voor werken op afstand, hybride of uitbestede omgevingen, en waarborgt bescherming en zichtbaarheid, ook wanneer bedrijfsmiddelen zich niet fysiek op locaties van de organisatie bevinden.

3. Doelstellingen

3.1 Het bijhouden van een volledige, nauwkeurige en actuele inventaris van alle informatieactiva van de organisatie, met vastgelegde kenmerken voor eigenaarschap, classificatie en locatie.

3.2 Het aanwijzen van bedrijfsmiddeleigenaren die verantwoordelijk zijn voor de classificatie, behandeling en bescherming van de bedrijfsmiddelen onder hun beheer, in overeenstemming met het beleid voor gegevensgovernance en informatiebeveiliging.

3.3 Het toepassen van passende classificatie en etikettering op alle bedrijfsmiddelen op basis van sensitiviteit, criticaliteit en regelgevende overwegingen.

3.4 Het beschermen van bedrijfsmiddelen overeenkomstig hun classificatie en bijbehorende risicoblootstelling, met inbegrip van opslag, toegang, overdracht en afvoer.

3.5 Het afdwingen van procedures voor teruggave van activa en veilige afvoer bij offboarding van medewerkers, beëindiging van contracten of het einde van de levenscyclus van bedrijfsmiddelen.

3.6 Het ondersteunen van naleving van kaders zoals ISO/IEC 27001, AVG, NIS2, DORA en COBIT 2019 door middel van gestructureerd beheer van bedrijfsmiddelen en audittrail.

4. Rollen en verantwoordelijkheden

4.1 Directie

4.1.1 Keurt het beleid inzake beheer van bedrijfsmiddelen goed en zorgt ervoor dat middelen beschikbaar worden gesteld voor de volledige implementatie ervan.

4.1.2 Draagt de eindverantwoordelijkheid om ervoor te zorgen dat bedrijfsmiddelen van de organisatie worden beschermd en beheerd in overeenstemming met wettelijke, regelgevende en contractuele verplichtingen.

4.2 Chief Information Security Officer (CISO)

4.2.1 Is eigenaar van dit beleid inzake beheer van bedrijfsmiddelen en waarborgt integratie met het bredere managementsysteem voor informatiebeveiliging (ISMS) van de organisatie.

4.2.2 Beoordeelt uitzonderingen en afwijkingen op dit beleid en stelt risicogebaseerde mitigerende maatregelen verplicht.

4.2.3 Houdt toezicht op periodieke audits van activaclassificatie, de integriteit van de inventaris van bedrijfsmiddelen en naleving van de levenscyclus van bedrijfsmiddelen.

[... 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 herzien, of naar aanleiding van:

9.1.1 wijzigingen in wettelijke of regelgevende verplichtingen die van invloed zijn op classificatie van bedrijfsmiddelen of vereisten voor inventarisatie

9.1.2 introductie van nieuwe categorieën bedrijfsmiddelen of beheerplatforms (bijvoorbeeld cloud-native CMDB's)

9.1.3 bevindingen uit interne audits of beveiligingsincidenten waarbij sprake is van onjuist beheer van bedrijfsmiddelen

9.1.4 organisatorische herstructurering die invloed heeft op eigenaarschap of beheersmaatregelen voor de levenscyclus

9.2 Het herzieningsproces moet worden gestart door de IT Asset Manager en worden gecoördineerd met de CISO, Inkoop, Juridische Zaken en Compliance en de betrokken afdelingshoofden.

9.3 Tussentijdse herzieningen kunnen ook worden geactiveerd door:

9.3.1 acquisitie of afstoting van bedrijfseenheden

9.3.2 leverancierswijzigingen die gevolgen hebben voor door derden beheerde bedrijfsmiddelen

9.3.3 technologische vernieuwingen waarbij sprake is van grootschalige buitengebruikstelling of toegangsverlening

9.4 Alle herzieningen van dit beleid moeten:

9.4.1 onder versiebeheer staan en worden opgeslagen in de ISMS-repository

9.4.2 worden goedgekeurd door de directie

9.4.3 een samenvatting van wijzigingen en onderbouwing bevatten

9.4.4 worden gecommuniceerd aan alle betrokken stakeholders, met inbegrip van bijgewerkte procedures of systeemtraining, waar van toepassing

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid functioneert in samenhang met en ondersteunt de handhaving van de volgende gerelateerde beleidslijnen:

10.1.1 P4 - Beleid inzake toegangsbeheersing: Waarborgt dat zichtbaarheid van bedrijfsmiddelen in lijn is met toegekende toegangsrechten en beheersmaatregelen binnen systemen en gegevensomgevingen.

10.1.2 P7 - Onboarding- en offboardingbeleid: Regelt tijdige toegangsverlening en teruggave van fysieke en logische bedrijfsmiddelen tijdens personele overgangen.

10.1.3 P13 - Beleid inzake gegevensclassificatie en etikettering: Stelt verplichte classificatieregels vast voor bedrijfsmiddelen die de procedures voor etikettering, behandeling en afvoer bepalen.

10.1.4 P14 - Beleid inzake gegevensbewaring en afvoer: Definieert de termijnen en methoden voor veilige afvoer van digitale en fysieke bedrijfsmiddelen die informatie bevatten.

10.1.5 P22 - Logging- en monitoringbeleid: Maakt traceerbaarheid van toegang tot en gebruik van bedrijfsmiddelen mogelijk via systeemlogging, endpointzichtbaarheid en gedragsanalyse.

10.1.6 P30 - Incidentresponsbeleid (P30): Ondersteunt snelle indamming en onderzoek van inbreuken met betrekking tot bedrijfsmiddelen, zoals verloren laptops of niet-getraceerde opslagmedia.

10.2 Deze beleidslijnen vormen samen een samenhangende governancestructuur die waarborgt dat bedrijfsmiddelen gedurende hun levenscyclus veilig worden beheerd, nauwkeurig worden geïnventariseerd en passend worden behandeld.

11. Referentienormen en -raamwerken

11.1 Dit beleid is afgestemd op internationaal erkende normen voor informatiebeveiliging en regelgevende kaders die robuust beheer van bedrijfsmiddelen gedurende de volledige levenscyclus vereisen.

11.2 ISO/IEC 27001:

11.2.1 Clausule 8.1 - Vereist dat organisaties de processen plannen, implementeren en beheersen die nodig zijn om aan informatiebeveiligingsvereisten te voldoen, waaronder die voor levenscyclusbeheer van bedrijfsmiddelen.

11.3 ISO/IEC 27002:2022 - Beheersmaatregelen 5.9 tot 5.11

11.3.1 Clausule 5.9 - Inventaris van informatie en andere bijbehorende activa: Vereist een actuele en volledige inventaris van alle bedrijfsmiddelen die relevant zijn voor informatieverwerking.

11.3.2 Clausule 5.10 - Aanvaardbaar gebruik van informatie en bedrijfsmiddelen: Ondersteund door gebruiksregels, eigenaarschap en processen voor teruggave.

11.3.3 Clausule 5.11 - Teruggave van activa: Geïmplementeerd via formele overdrachts- en buitengebruikstellingsprocedures.

11.3.4 Deze beheersmaatregelen stellen gestructureerde vereisten vast voor het identificeren, etiketteren, onderhouden en volgen van bedrijfsmiddelen van de organisatie, met bijbehorende verantwoordelijkheden voor eigenaren en beheerders gedurende de levenscyclus.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - Inventaris van systeemcomponenten: Komt tot uiting in gecentraliseerd beheer van bedrijfsmiddelen, realtime zichtbaarheid en koppeling met operationele configuraties.

11.4.2 RA-3 - Risicobeoordeling: Inventarissen van bedrijfsmiddelen vormen een basiselement voor dreigingsmodellering en risicobeoordeling.

11.4.3 MP-6 - Mediasanering: Afgedwongen via veilige afvoermethoden zoals vastgelegd in beheersmaatregelen voor de levenscyclus van bedrijfsmiddelen en het beleid inzake gegevensafvoer.

11.5 EU AVG (2016/679):

11.5.1 Artikel 30 - Verwerkingsregister: Vereist dat organisaties systemen, apparaten en opslaglocaties documenteren waarin persoonsgegevens worden opgeslagen of verwerkt.

11.5.2 Artikel 32 - Beveiliging van verwerking: Sluit aan op risicobeoordeling op basis van bedrijfsmiddelen en beheersmaatregelen die zijn afgestemd op geclassificeerde bedrijfsmiddelen en kritieke infrastructuur.

11.6 EU NIS2-richtlijn (2022/2555):

11.6.1 Artikel 21(2)(a, b): Verplicht zichtbaarheid op en inventarisatie van bedrijfsmiddelen als basis voor risicoanalyse, bescherming en respons op cyberbeveiligingsincidenten.

11.6.2 Artikel 21(3): Bekrachtigt de noodzaak van gestructureerde governance van bedrijfsmiddelen als onderdeel van een organisatorische beveiligingscultuur.

11.7 EU DORA (2022/2554):

11.7.1 Artikel 5 - ICT-governance en interne beheersing: Vereist dat financiële entiteiten ICT-bedrijfsmiddelen beheersen met duidelijke vereisten voor inventarisatie, eigenaarschap en bescherming.

11.7.2 Artikel 9 - ICT-risicobeheerkader: Bepaalt dat processen voor beheer van bedrijfsmiddelen dreigingsmitigatie, continuïteitsplanning en operationele weerbaarheid moeten ondersteunen.

11.8 COBIT 2019:

11.8.1 BAI09 - Beheer van bedrijfsmiddelen: Sluit rechtstreeks aan op de gestructureerde identificatie, classificatie, het gebruik en de afvoer van bedrijfsmiddelen binnen de onderneming.

11.8.2 DSS01 - Beheerde operaties: Ondersteunt de implementatie van beheersmaatregelen die bescherming van bedrijfsmiddelen en continue operationele governance waarborgen.

11.8.3 MEA03 - Monitoren, evalueren en beoordelen van naleving: Waarborgt regelmatige auditing van beheersmaatregelen voor beheer van bedrijfsmiddelen en de doeltreffendheid daarvan voor afstemming op regelgeving.