					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P12S					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**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 8	Vereisten voor beheer van bedrijfsmiddelen
ISO/IEC 27002:2022	Beheersmaatregel 5	Beheersmaatregelen voor beheer van bedrijfsmiddelen
NIST SP 800-53 Rev.5	CM-8	Inventaris van systeemcomponenten
EU NIS2	Artikel 21(2)(a)	Registratie van bedrijfsmiddelen ter bescherming van netwerk- en informatiesystemen
EU DORA	Artikel 5(8)	Vereisten voor de inventarisatie van ICT-activa
COBIT 2019	BAI	Levenscyclusbeheer van IT-activa
AVG	Artikel 30	Register van verwerkingsactiviteiten

1. Doel

1.1 Dit beleid bepaalt hoe de organisatie haar informatieactiva identificeert, registreert, beschermt en buiten gebruik stelt, met inbegrip van zowel fysieke als digitale componenten.

1.2 Het doel is operationele risico's en beveiligingsrisico's te beperken door gedurende de volledige levenscyclus van alle bedrijfsmiddelen zichtbaarheid, verantwoordelijkheid en veilige omgang te waarborgen.

1.3 Een betrouwbare inventaris van bedrijfsmiddelen ondersteunt naleving van wet- en regelgeving, incidentrespons, continuïteitsplanning en risicobeheer.

1.4 Dit beleid ondersteunt tevens certificering volgens ISO/IEC 27001 en toont afstemming aan met juridische, financiële en cyberbeveiligingsverplichtingen onder kaders zoals de AVG, NIS2 en DORA.

1.5 Voor het mkb is een eenvoudige maar systematische aanpak van beheer van bedrijfsmiddelen essentieel om onbeheerde apparaten, gegevensverlies of tekortkomingen tijdens audits te voorkomen, in het bijzonder wanneer de technische personeelsbezetting beperkt is.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle bedrijfsmiddelen die eigendom zijn van, geleased worden door of anderszins door de organisatie worden beheerd, met inbegrip van bedrijfsmiddelen die worden gebruikt in:

2.1.1 kantooromgevingen

2.1.2 thuiswerk- of hybride werkomgevingen

2.1.3 veldwerk- of mobiele omgevingen

2.1.4 cloudomgevingen en uitbestede omgevingen

2.2 Onder de reikwijdte vallende typen bedrijfsmiddelen omvatten onder meer:

2.2.1 Hardware: laptops, desktops, monitoren, telefoons, tablets, USB-sticks, routers, printers, back-upmedia

2.2.2 Software: geïnstalleerde applicaties, SaaS-oplossingen, besturingssystemen, antivirussoftware, licenties

2.2.3 Gegevensactiva: opslaglocaties voor bedrijfsgegevens, spreadsheets, klantregistraties, broncode

2.2.4 Digitale middelen en diensten: domeinnamen, digitale certificaten, API-sleutels, e-mailaccounts, cloudtoegangsgegevens

2.2.5 Toegangsmiddelen: sleutels, smartcards, toegangspassen, biometrische tokens

2.3 Alle werknemers, opdrachtnemers en externe dienstverleners die bedrijfsmiddelen van de organisatie verwerken, vallen onder de reikwijdte van dit beleid.

2.4 Dit beleid is tevens van toepassing op zowel kortlopende bedrijfsmiddelen (bijvoorbeeld projectspecifieke laptops) als langlopende bedrijfsmiddelen, alsook op gedeelde bedrijfsmiddelen die door meerdere medewerkers worden gebruikt.

3. Doelstellingen

3.1 Een volledige en nauwkeurige inventaris van bedrijfsmiddelen opzetten en onderhouden voor alle relevante bedrijfsmiddelen, die doorlopend wordt bijgewerkt.

3.2 Waarborgen dat elk bedrijfsmiddel een aangewezen eigenaar heeft die verantwoordelijk is voor het gebruik, de opslag en de teruggave ervan.

3.3 Bedrijfsmiddelen classificeren op basis van gevoeligheid, bedrijfsimpact of relevantie vanuit wet- en regelgeving, zodat gedifferentieerde beschermingsniveaus kunnen worden toegepast.

3.4 Duidelijke procedures vaststellen voor uitgifte, hertoewijzing, onderhoud, melding van verlies en buitengebruikstelling van bedrijfsmiddelen.

3.5 Waarborgen dat bedrijfsmiddelen gedurende hun volledige levenscyclus veilig worden behandeld en dat de informatie die zij opslaan bij afvoer wordt beschermd of veilig wordt gewist.

3.6 De kans op beveiligingsincidenten als gevolg van niet-geregistreerde, niet-ingeleverde of onjuist gebruikte bedrijfsmiddelen verminderen.

3.7 Ondersteuning bieden voor naleving van toepasselijke wet- en regelgeving (zoals het verantwoordingsbeginsel van de AVG) en normen voor cyberbeveiligingscertificering.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Is eigenaar van dit beleid en is verantwoordelijk voor het waarborgen dat beheermaatregelen voor bedrijfsmiddelen organisatiebreed worden geïmplementeerd en nageleefd.

4.1.2 Beoordeelt en keurt actualisaties van de inventaris van bedrijfsmiddelen goed en autoriseert waar nodig de buitengebruikstelling of overdracht van bedrijfsmiddelen.

4.1.3 Wordt geïnformeerd over ieder significant verlies, iedere diefstal of ieder misbruik van bedrijfsmiddelen.

4.2 IT-verantwoordelijke of aangewezen beheerder van bedrijfsmiddelen

4.2.1 Beheert de inventaris van bedrijfsmiddelen (bijvoorbeeld in een spreadsheet, helpdesksysteem of lichtgewicht assetmanagementtool).

4.2.2 Wijst eigenaarschap van bedrijfsmiddelen toe en registreert statuswijzigingen (bijvoorbeeld nieuw, in gebruik, in reparatie, buiten gebruik).

4.2.3 Verifieert dat alle uitgegeven bedrijfsmiddelen zijn gedocumenteerd en gekoppeld aan een individu of bedrijfseenheid.

4.2.4 Zorgt ervoor dat classificatielabels worden toegepast en nageleefd (bijvoorbeeld Intern, Vertrouwelijk).

4.2.5 Coördineert de inname, veilige gegevenswissing en deactivering van bedrijfsmiddelen tijdens uitdiensttreding of buitengebruikstelling.

4.2.6 Rapporteert onopgeloste afwijkingen in de registratie van bedrijfsmiddelen aan de GM.

[... 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 actualisatie

9.1 Dit beleid wordt ten minste eenmaal per jaar herzien en daarnaast telkens wanneer:

9.1.1 nieuwe typen technologie of bedrijfsmiddelen worden geïntroduceerd

9.1.2 procedures voor het registreren van bedrijfsmiddelen wijzigen (bijvoorbeeld door invoering van nieuwe tools of platforms)

9.1.3 nieuwe wettelijke of reglementaire verplichtingen gevolgen hebben voor traceerbaarheid of afvoer van bedrijfsmiddelen

9.1.4 een incident of audit een tekortkoming in de huidige beheerpraktijken voor bedrijfsmiddelen identificeert

9.2 Bij herzieningen worden de GM en de IT-verantwoordelijke betrokken en worden procedures voor omgang met bedrijfsmiddelen, inventarissjablonen en richtlijnen voor classificatie waar nodig geactualiseerd.

9.3 Alle actualisaties worden gedocumenteerd en gecommuniceerd aan betrokken medewerkers. Een wijzigingslogboek onder versiebeheer wordt bijgehouden.

10. Gerelateerde beleidsdocumenten en samenhang

10.1 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: wijst verantwoordelijkheden toe voor beleidseigenaarschap en IT-operaties.

10.2 P4S – Beleid inzake toegangsbeveiliging: verbindt het gebruik van bedrijfsmiddelen (bijvoorbeeld laptops, mobiele apparaten) aan toegangsrechten van gebruikers en identiteitsbeheer.

10.3 P7S – Onboarding- en offboardingbeleid: borgt dat uitgifte en terugname van bedrijfsmiddelen zijn ingebed in HR-processen gedurende de personeelslevenscyclus.

10.4 P13S – Beleid inzake gegevensclassificatie en etikettering: biedt regels om vast te stellen of een bedrijfsmiddel als Intern of Vertrouwelijk moet worden geclassificeerd.

10.5 P30S – Incidentresponsbeleid: beschrijft responsprocedures indien een gebeurtenis met betrekking tot bedrijfsmiddelen leidt tot een beveiligings- of privacy-incident.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 8.1: vereist operationele beheersmaatregelen om bedrijfsmiddelen te beheren en deze gedurende het gebruik te beschermen.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 5.9: beschrijft hoe bedrijfsmiddelen moeten worden geïdentificeerd, van eigenaarschap voorzien, geclassificeerd en veilig beheerd.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-8: vereist dat organisaties een inventaris van systeemcomponenten ontwikkelen en onderhouden, met inbegrip van hardware, software en virtuele activa.

11.4 AVG

11.4.1 Artikel 30: vereist documentatie van verwerkingsactiviteiten, wat afhankelijk is van inzicht in waar gegevens zijn opgeslagen en op welke bedrijfsmiddelen.

11.5 EU NIS2

11.5.1 Artikel 21(2)(a): verlangt technische en organisatorische maatregelen, waaronder registratie van bedrijfsmiddelen, ter bescherming van netwerk- en informatiesystemen.

11.6 EU DORA

11.6.1 Artikel 5(8): financiële entiteiten moeten gedetailleerde inventarissen van ICT-activa bijhouden als onderdeel van ICT-risicobeheer.

11.7 COBIT 2019

11.7.1 BAI09: bepaalt dat IT-activa gedurende hun volledige levenscyclus moeten worden beheerd — van verwerving tot buitengebruikstelling — met duidelijk eigenaarschap en beheersmaatregelen.