					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P04					Documenttitel: **Beleid inzake toegangscontrole**							
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	Clausules 5.15, 5.17, 5.18	Logische en fysieke toegangsbeheersing
ISO/IEC 27002:2022	Beheersmaatregelen 8.2, 8.3	Rolgebaseerde toegang en identiteitsbeheer
NIST SP 800-53 Rev.5	AC-1 t/m AC-20, IA-1 t/m IA-8	Beheersmaatregelen voor account- en toegangsbeheer, identiteitsauthenticatie
EU AVG	Artikelen 5(1)(f), 32(1)(b); overweging 39	Gegevensbescherming en gegevensminimalisatie
EU NIS2	Artikel 21(2)(c–e)	Toegangs- en gebruikersauthenticatie en bescherming van bedrijfsmiddelen
EU DORA	Artikelen 6, 9(2)	ICT- en gebruikerstoegang en sterke beheersmaatregelen voor derde partijen
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Onboarding, operatie, monitoring, naleving

1. Doel

1.1 Dit beleid stelt verplichte principes, verantwoordelijkheden en beheersingsvereisten vast voor het beheren van toegang tot informatiesystemen, applicaties, fysieke faciliteiten en informatieactiva binnen de organisatie.

1.2 Het waarborgt dat toegang wordt verleend op basis van zakelijke noodzaak, functie en risicoprofiel, met toepassing van principes zoals het least-privilegebeginsel, het need-to-know-principe en functiescheiding (SoD).

1.3 Dit beleid ondersteunt de implementatie van ISO/IEC 27001:2022, clausule 5.15, en gerelateerde beheersmaatregelen voor logische en fysieke toegang, gebruikersauthenticatie en beheer van de toegangslevenscyclus.

1.4 Dit beleid ondersteunt de bescherming van digitale en fysieke middelen tegen ongeautoriseerd gebruik, misbruik of compromittering.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle gebruikers, systemen en faciliteiten binnen de scope van het ISMS, waaronder:

2.1.1 werknemers, opdrachtnemers, leveranciers en tijdelijk personeel

2.1.2 on-premises infrastructuur, cloudgehoste systemen en hybride omgevingen

2.1.3 alle bedrijfsactiva — hardware, software, gegevens en beveiligde gebieden

2.1.4 logische toegang (bijvoorbeeld systemen, netwerken, applicaties, API's) en fysieke toegang (bijvoorbeeld gebouwen, datacenters)

2.2 Het regelt toegang gedurende de volledige levenscyclus van identiteiten en interactie met middelen, van onboarding en toegangsverlening tot functiewijzigingen en uitdiensttreding.

2.3 Het beleid omvat ook Bring Your Own Device (BYOD) en externe toegang (VPN, beheer van mobiele apparaten), en waarborgt dat beheersmaatregelen consistent zijn over locaties en eigendomsmodellen van apparaten heen.

3. Doelstellingen

3.1 Het implementeren van veilige, rolgebaseerde toegangsbeheersmaatregelen die operationele integriteit en naleving van wet- en regelgeving ondersteunen.

3.2 Waarborgen dat toegangsrechten passend worden goedgekeurd, gemonitord en tijdig worden ingetrokken.

3.3 Voorkomen van ongeautoriseerde toegang, privilege-escalatie of het voortbestaan van verouderde toegangsrechten.

3.4 Ondersteunen van zero-trustprincipes door toegang standaard te weigeren, tenzij deze expliciet is goedgekeurd en gemotiveerd.

3.5 Assurance bieden aan auditors en stakeholders door middel van op bewijsmateriaal gebaseerde, geautomatiseerde toegangsbeoordelingen en beleidsafdwinging.

3.6 Toegangscontrole verankeren in bedrijfsprocessen, HR-processen en technische architecturen.

4. Rollen en verantwoordelijkheden

4.1 Topmanagement

4.1.1 Bekrachtigt het Beleid inzake toegangscontrole en zorgt voor passend budget en voldoende capaciteit voor de handhaving ervan.

4.1.2 Beoordeelt toegangscontrolerisico's tijdens managementbeoordelingen en wijst op strategisch niveau eigenaarschap en verantwoording toe.

4.2 CISO / ISMS-manager

4.2.1 Is eigenaar van het toegangscontrolekader en waarborgt afstemming met ISO/IEC 27001 en gerelateerde normen.

4.2.2 Coördineert beleidsafdwinging, toetsing en remediatie van beheersmaatregelen en rapportage over toegangscontrolemetrieken.

4.2.3 Houdt toezicht op risicogebaseerde toegangsmodellering en bewaakt structurele hiaten in de beheersing.

[... 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 Triggers en frequentie van herziening

9.1.1 Dit beleid moet worden herzien:

9.1.1.1 jaarlijks, of

9.1.1.2 na een ingrijpende wijziging in de IT-infrastructuur, regelgevingseisen of het risicoprofiel

9.1.1.3 na incidenten die zwakheden in toegangsbeheersmaatregelen aan het licht brengen

9.1.1.4 wanneer significante wijzigingen optreden in authenticatietechnologieën of identiteitsplatforms

9.2 Bevoegdheid en proces voor herziening

9.2.1 De CISO of aangewezen ISMS-verantwoordelijke beheert de herzieningscyclus en betrekt daarbij:

9.2.1.1 bevindingen van interne audits

9.2.1.2 resultaten en metrieken van toegangsbeoordelingen

9.2.1.3 juridische en regelgevende actualisaties

9.2.1.4 wijzigingen in technologieplatforms

9.2.2 Alle revisies moeten worden goedgekeurd door het topmanagement en worden gecommuniceerd aan alle stakeholders.

9.2.3 Van betrokken gebruikers kan worden verlangd dat zij bij materiële wijzigingen opnieuw kennisneming van het beleid bevestigen.

9.3 Versiebeheer en documentatie

9.3.1 De masterversie moet worden opgeslagen in de ISMS-documentrepository met de volgende metadata:

9.3.1.1 versienummer en wijzigingslogboek

9.3.1.2 ingangsdatum en datum van volgende herziening

9.3.1.3 eigenaar en goedkeuringsbevoegdheid

9.3.1.4 distributie- en kennisnameregistraties

9.3.2 Vervangen versies moeten worden gearchiveerd en gedurende ten minste 3 jaar toegankelijk blijven.

10. Gerelateerde beleidsdocumenten en samenhang

10.1 Dit beleid is functioneel afhankelijk van, en moet worden geïnterpreteerd in samenhang met:

10.1.1 P01 – Informatiebeveiligingsbeleid: definieert de beveiligingstoezegging van de organisatie en de overkoepelende verwachtingen voor toegangscontrole.

10.1.2 P03 – Beleid inzake aanvaardbaar gebruik: stelt gedragsvoorwaarden vast voor toegang en verantwoordingsplicht van gebruikers voor verantwoord systeemgebruik.

10.1.3 P05 – Wijzigingsbeheerbeleid: regelt hoe wijzigingen in toegangsconfiguraties, rollen of groepsstructuren veilig moeten worden geïmplementeerd en getest.

10.1.4 P07 – Onboarding- en offboardingbeleid: stuurt de toekenning en intrekking van toegangsrechten aan in overeenstemming met gebeurtenissen in de gebruikerslevenscyclus.

10.1.5 P11 – Beleid inzake gebruikersaccounts en privilegebeheer: operationaliseert beheersmaatregelen op accountniveau en vult dit beleid aan met richtlijnen voor technische afdwinging van toegang.

10.2 Gezamenlijk bieden deze beleidsdocumenten een samenhangend en afdwingbaar governancekader voor toegang binnen bedrijfsonderdelen en technologieën.

11. Referentienormen en raamwerken

11.1 ISO/IEC 27001:2022:

11.1.1 Clausule 5.15 – Toegangscontrole: dit beleid geeft invulling aan de eis om toegang tot informatie en andere gerelateerde activa te beheersen op basis van zakelijke en informatiebeveiligingsvereisten.

11.1.2 Clausule 5.17 – Identiteitsbeheer en clausule 5.18 – Authenticatie-informatie: deze worden geoperationaliseerd via identiteitsprovisioning, authenticatiemechanismen en toewijzing van privileges.

11.1.3 Bijlage A, beheersmaatregelen 8.2 (Beleid inzake toegangscontrole) en 8.3 (Identiteitsbeheer): vormen de basis voor de doelstellingen van de beheersmaatregelen in dit beleid, waaronder rolgebaseerde toegang, integratie van de identiteitslevenscyclus en bescherming van geprivilegieerde toegang.

11.2 NIST SP 800-53 Rev.5:

11.2.1 AC-familie (AC-1 t/m AC-20): dit beleid ondersteunt de NIST-vereisten voor toegangscontrole voor zowel fysieke als logische systemen, waaronder beleidsdefinitie (AC-1), accountbeheer (AC-2) en functiescheiding (SoD) (AC-5).

11.2.2 IA-familie (IA-1 t/m IA-8): biedt richtlijnen voor identiteitsauthenticatie, bescherming van referenties en MFA.

11.2.3 AU-2, AU-12: de vereisten voor logging en auditing die onder dit beleid worden afgedwongen, ondersteunen gebruikersverantwoordelijkheid en incidentonderzoek.

11.2.4 PE-2 t/m PE-6: adresseren beperkingen op fysieke toegang, die door dit beleid gedeeltelijk worden afgedwongen via beheersmaatregelen voor badges en toegangsrechten voor gebouwen.

11.3 EU AVG (2016/679):

11.3.1 Artikel 5(1)(f): persoonsgegevens moeten worden beschermd tegen ongeautoriseerde toegang. Dit beleid waarborgt de technische en procedurele afdwinging van dat beginsel.

11.3.2 Artikel 32(1)(b): vereist de implementatie van toegangsbeheersmaatregelen, pseudonimisering en encryptie om ongeautoriseerde verwerking van persoonsgegevens te voorkomen.

11.3.3 Overweging 39: schrijft minimalisering van toegang tot persoonsgegevens voor, hier afgedwongen via minimale bevoegdheden en vereisten voor onderbouwing van toegang.

11.4 EU NIS2-richtlijn (2022/2555):

11.4.1 Artikel 21(2)(c–e): dit beleid maakt technische en organisatorische maatregelen mogelijk voor toegangscontrole, gebruikersauthenticatie en bescherming van bedrijfsmiddelen bij essentiële en belangrijke entiteiten.

11.5 EU DORA (2022/2554):

11.5.1 Artikel 6: vereist ICT-risicobeheerbeleid dat uitdrukkelijk beheer van gebruikerstoegang en beheersmaatregelen voor de identiteitslevenscyclus omvat. Dit beleid voldoet aan die eis voor de financiële sector en de ICT-dienstensector.

11.5.2 Artikel 9(2): dit beleid ondersteunt de handhaving van sterke toegangsbeheersmaatregelen als onderdeel van ICT-dienstbeheer van derden en binnen de groep.

11.6 COBIT 2019:

11.6.1 APO07 – Managed Human Resources: handhaaft onboarding- en offboardingbeheersmaatregelen ter ondersteuning van governance van toegang.

11.6.2 BAI03 – Managed Solutions Identification and Build: verankert vereisten voor toegangscontrole in systeemontwerp en wijzigingsprocessen.

11.6.3 DSS01 – Managed Operations en DSS05 – Managed Security Services: regelen de handhaving van beperkingen op logische toegang en monitoring van overtredingen.

11.6.4 MEA03 – Monitoren, evalueren en beoordelen van naleving: ondersteunt audit- en assurancemechanismen voor de validatie van de effectiviteit van toegangsbeheersmaatregelen.