					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P04S					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	Clausule 5	
ISO/IEC 27002:2022	Beheersmaatregelen 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1 tot en met AC-5	
AVG	Artikel 32	
EU NIS2	Artikel 21(2)(b)	
EU DORA	Artikel 9	
COBIT 2019	APO07, DSS01	

1. Doel

1.1. Dit beleid bepaalt hoe de organisatie de toegang tot systemen, gegevens en faciliteiten beheert om te waarborgen dat uitsluitend geautoriseerde personen op basis van een zakelijke noodzaak toegang hebben tot informatie.

1.2. Het stelt duidelijke regels vast voor het verlenen, wijzigen, monitoren en intrekken van gebruikerstoegang om het risico op ongeautoriseerde toegang te beperken en de naleving van toepasselijke wet- en regelgeving en normen te ondersteunen.

1.3. Dit beleid dwingt het principe van minimale bevoegdheden af, waarbij toegang wordt beperkt tot het minimum dat nodig is om werkzaamheden uit te voeren.

2. Reikwijdte

2.1. Dit beleid is van toepassing op alle personen die toegang gebruiken tot of beheren voor de IT-systemen, netwerken, gegevens of faciliteiten van de organisatie, waaronder:

2.1.1. Werknemers

2.1.2. Contractanten

2.1.3. Tijdelijke medewerkers

2.1.4. Externe IT-dienstverleners

2.2. Het beleid heeft betrekking op toegang tot:

2.2.1. Bedrijfstoepassingen, bestandsshares en databases

2.2.2. E-mail-, VPN- en systemen voor toegang op afstand

2.2.3. Cloudgebaseerde diensten die voor bedrijfsdoeleinden worden gebruikt

2.2.4. Fysieke toegang tot beveiligde ruimten, zoals kantoren of serverruimten

2.3. Dit beleid is afdwingbaar voor alle apparaten (door de organisatie verstrekt of goedgekeurde Bring Your Own Device (BYOD)), platforms en locaties.

3. Doelstellingen

3.1. Waarborgen dat toegangsrechten uitsluitend worden toegekend na formele goedkeuring op basis van rol en zakelijke rechtvaardiging.

3.2. Voorkomen van ongeautoriseerde of bovenmatige toegang tot gevoelige gegevens, systemen of infrastructuur.

3.3. Vaststellen van duidelijke procedures voor het verlenen, wijzigen en beëindigen van gebruikerstoegang.

3.4. Verplichten van periodieke beoordelingen van toegangsrechten en geautomatiseerde of handmatige logging ter ondersteuning van audits.

3.5. Ondersteunen van technische afdwinging van toegangsbeperkingen door middel van configuratie en monitoring.

4. Rollen en verantwoordelijkheden

4.1. Algemeen directeur

4.1.1. Keurt dit beleid goed en zorgt ervoor dat middelen beschikbaar zijn om doeltreffende beheersmaatregelen voor toegangscontrole te implementeren.

4.1.2. Keurt uitzonderingen goed en beoordeelt jaarlijkse toegangsaudits.

4.2. IT-manager / Externe IT-dienstverlener

4.2.1. Verzorgt het verlenen, wijzigen en beëindigen van gebruikersaccounts.

4.2.2. Beheert een register voor toegangscontrole met alle activiteiten met betrekking tot aanmaak, wijzigingen en verwijderingen.

4.2.3. Implementeert rolgebaseerde toegangscontrole (RBAC) en dwingt sterke authenticatie af, zoals MFA.

4.2.4. Beoordeelt logbestanden van toegangscontrole op verdachte activiteiten en rapporteert bevindingen aan de algemeen directeur.

[... 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. Jaarlijkse beleidsbeoordeling

9.1.1. De IT-manager moet dit beleid jaarlijks beoordelen. Wijzigingen in de juridische, technische of organisatorische context moeten leiden tot onmiddellijke actualisering.

9.2. Triggers voor beoordeling

9.2.1. Het beleid moet ook worden beoordeeld als zich een van de volgende situaties voordoet:

9.2.2. Grote systeemwijzigingen of migraties naar cloudgehoste systemen

9.2.3. Wijzigingen in rollen of organisatiestructuur

9.2.4. Een beveiligingsincident met ongeautoriseerde toegang

9.2.5. Wijzigingen in regelgeving, bijvoorbeeld updates van de AVG, NIS2 of DORA

9.3. Documenteren en communiceren van wijzigingen

9.3.1. Herzieningen moeten worden geregistreerd met versiehistorie, goedkeuring door de algemeen directeur en communicatie aan alle betrokken medewerkers.

9.4. Toegankelijkheid en training

9.4.1. Dit beleid moet beschikbaar worden gesteld aan alle medewerkers en relevante training moet worden verzorgd als onderdeel van onboarding en vervolgens jaarlijks.

10. Gerelateerde beleidsdocumenten en samenhang

10.1. Dit beleid moet in samenhang met de volgende SME-beleidsdocumenten worden toegepast om veilige toegangspraktijken volledig af te dwingen:

10.1.1. P3S – Beleid inzake aanvaardbaar gebruik: zorgt ervoor dat gebruikers begrijpen welk gedrag aanvaardbaar is bij verleende toegang.

10.1.2. P5S – Wijzigingsbeheerbeleid: zorgt ervoor dat toegangsrechten zijn afgestemd op goedgekeurde systeemwijzigingen.

10.1.3. P7S – Onboarding- en offboardingbeleid: definieert de triggerpunten voor toegangsverlening en het intrekken van gebruikerstoegang.

10.1.4. P17S – Beleid inzake gegevensbescherming en privacy: zorgt ervoor dat beheersmaatregelen voor toegangscontrole aansluiten op waarborgen voor persoonsgegevens.

10.1.5. P30S – Incidentresponsbeleid (P30): definieert hoe toegangsgerelateerde incidenten, zoals misbruik of inbreuken, worden beheerd en onderzocht.

11. Referentienormen en -kaders

11.1. ISO/IEC 27001

11.1.1. Beheersmaatregel 5.15 – Vereist geformaliseerd beleid en processen voor toegangscontrole.

11.2. ISO/IEC 27002

11.2.1. Beheersmaatregelen 5.15–5.17 – Geven gedetailleerde richtlijnen voor rolgebaseerde toegang, integratie van de identiteitslevenscyclus en het beheer van geprivilegieerde toegang.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 tot en met AC-5 – Vereisen gestructureerd beleid voor toegangsbeheer, waaronder autorisatie van accounts, beoordeling en monitoring.

11.4. AVG

11.4.1. Artikel 32 – Vereist technische en organisatorische beheersmaatregelen, zoals toegangsbeheer, om gegevensbeveiliging en vertrouwelijkheid te waarborgen.

11.5. EU NIS2-richtlijn

11.5.1. Artikel 21(2)(b) – Verplicht operationele toegangscontrole en identiteitsbeheersystemen om ongeautoriseerde toegang tot systemen te voorkomen.

11.6. EU DORA

11.6.1. Artikel 9 – Benadrukt het veilige beheer van ICT-risico's, inclusief robuuste toegangscontrole voor financiële entiteiten.

11.7. COBIT 2019

11.7.1. APO07 – Managed Human Resources: vereist gedefinieerde en afgedwongen verantwoordelijkheden voor toegang.

11.7.2. DSS01 – Managed Operations: omvat procedures voor het beheren van logische toegang en het in stand houden van veilige operationele omgevingen.