| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Voer hier de naam van de geregistreerde rechtspersoon in | | | | | | |
| Documentnummer:<br>P11 | | | | | Documenttitel:<br>**Beleid inzake beheer van gebruikersaccounts en rechten** | | | | | | |
| 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 | Clausule 6.1.3, Clausule 8 | - |
| ISO/IEC 27002:2022 | Beheersmaatregelen 5.15-5.18 | - |
| NIST SP 800-53 Rev.5 | AC-1, AC-2, AC-5, AC-6, IA-2 t/m IA-5, AU-2, AU-12 | - |
| AVG | Artikelen 5(1)(f), 32; overweging 39 | - |
| EU NIS2 | Artikelen 21(2)(a, d), 21(3) | - |
| EU DORA | Artikelen 5, 9 | - |
| COBIT 2019 | DSS01, DSS05, APO13 | - |

**1. Doel**

**1 Dit beleid stelt verplichte beheersmaatregelen vast voor het beheer van gebruikersaccounts en rechten binnen alle informatiesystemen en diensten. Het waarborgt dat toegang tot bedrijfsmiddelen wordt verleend op basis van een gevalideerde identiteit, noodzaak vanuit de rol en de beginselen van minimale bevoegdheden en functiescheiding (SoD).**

1.1 Het ondersteunt de inzet van de organisatie voor informatiebeveiliging door gestructureerde, auditeerbare processen vast te stellen voor toegangsverlening, toekenning van rechten, bewaking van gebruik en intrekking van toegangsrechten.

1.2 Dit beleid is van cruciaal belang voor het beperken van het risico op ongeautoriseerde toegang, misbruik van rechten, interne dreigingen en niet-naleving van toepasselijke wet- en regelgeving.

**2. Reikwijdte**

2.1 Dit beleid is van toepassing op alle werknemers, contractanten, externe dienstverleners, consultants en andere personen aan wie toegang wordt verleend tot de IT-middelen, applicaties of gegevens van de organisatie.

**2.2 Het beleid is van toepassing op alle systemen en omgevingen waarin gebruikersauthenticatie en toegangscontrolemechanismen worden toegepast, waaronder begrepen maar niet beperkt tot:**

2.2.1 Bedrijfsapplicaties en databases

2.2.2 Cloudplatforms en SaaS-omgevingen

2.2.3 Besturingssystemen en beheerdersconsoles

2.2.4 Voorzieningen voor externe toegang (VPN, beheer van mobiele apparaten)

2.2.5 Systemen voor identiteits- en toegangsbeheer (IAM)

**2.3 Het beleid omvat zowel standaardgebruikersaccounts als geprivilegieerde accounts en bevat beheersmaatregelen voor:**

2.3.1 Het aanmaken, wijzigen en deactiveren van accounts

2.3.2 Privilege-escalatie en delegatie

2.3.3 Sessiecontrole en monitoring

2.3.4 Authenticatiemethoden en beheer van authenticatiemiddelen

**3. Doelstellingen**

3.1 Waarborgen dat alle gebruikersaccounts uniek identificeerbaar zijn, correct geautoriseerd zijn en uitsluitend worden toegewezen na formele validatie van de noodzaak.

3.2 Het beginsel van minimale bevoegdheden toepassen en onnodige of buitensporige toegang voorkomen door strikte beheersmaatregelen af te dwingen voor de toekenning en het gebruik van geprivilegieerde accounts.

3.3 Vereisen dat de accountstatus tijdig wordt bijgewerkt op basis van wijzigingen in dienstverband of rol, met inbegrip van onmiddellijke deactivering bij uitdiensttreding.

3.4 Proactieve detectie en remediatie mogelijk maken van inactieve, misbruikte of ongeautoriseerde accounts via logging, beoordelingen en automatisering.

3.5 Afstemming behouden met ISO/IEC 27001:2022 en aanverwante normen en voldoen aan verplichtingen op grond van relevante wet- en regelgeving zoals de AVG, NIS2, DORA en COBIT 2019.

**4. Rollen en verantwoordelijkheden**

**4.1 Chief Information Security Officer (CISO)**

4.1.1 Is eigenaar van dit beleid en waarborgt de handhaving ervan binnen de organisatie.

4.1.2 Beoordeelt en keurt formele uitzonderingen of gevallen van noodtoegang goed.

4.1.3 Rapporteert auditbevindingen met betrekking tot accounts en escaleert risico's naar het hoger management.

**4.2 Manager toegangsbeheer / IT-beheerder**

4.2.1 Onderhoudt en beheert de technische beheersmaatregelen voor levenscyclusbeheer van gebruikersaccounts.

4.2.2 Voert toegangsverlening, intrekking van toegangsrechten en rechtenbeheer uit op basis van een goedgekeurde aanvraag.

4.2.3 Houdt een gezaghebbend register bij van alle gebruikersaccounts, hun status en hun rechtenniveau.

4.2.4 Ondersteunt audits en nalevingsbeoordelingen met logbestanden en activiteitenrapportages.

[ ... 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 Dit beleid moet ten minste jaarlijks worden beoordeeld of bij significante wijzigingen in:**

9.1.1 Organisatiestructuur of bedrijfsprocessen

9.1.2 IT-systemen, identiteitsplatforms of toegangsmethoden

9.1.3 Regelgevende of contractuele vereisten met betrekking tot identiteits- en toegangsbeheer

9.2 De Chief Information Security Officer (CISO) is samen met de manager toegangsbeheer verantwoordelijk voor het initiëren van het beoordelingsproces en het coördineren van feedback van stakeholders.

**9.3 Tussentijdse beoordelingen kunnen worden getriggerd door:**

9.3.1 Beveiligingsincidenten gerelateerd aan accountmisbruik

9.3.2 Auditbevindingen die tekortkomingen in het levenscyclusbeheer van accounts aan het licht brengen

9.3.3 Uitrol van nieuwe tools voor identiteitsbeheer of beheer van geprivilegieerde toegang (PAM)

**9.4 Actualisaties van dit beleid moeten:**

9.4.1 Onder versiebeheer staan en worden vastgelegd in de ISMS-documentatiebibliotheek

9.4.2 Worden gecommuniceerd aan alle relevante stakeholders, waaronder afdelingshoofden, IT-operatie en HR

9.4.3 Worden ondersteund door bijgewerkt opleidingsmateriaal en procedurele richtlijnen

9.5 Alle wijzigingen moeten worden goedgekeurd door het hoger management of de Stuurgroep Informatiebeveiliging (ISSC) en worden gelogd voor auditdoeleinden.

**10. Gerelateerde beleidslijnen en samenhang**

**10.1 Dit beleid is operationeel verbonden met en wordt ondersteund door de volgende gerelateerde beleidslijnen binnen de ISMS-suite:**

10.1.1 P4 Beleid inzake toegangscontrole: Stelt de overkoepelende beginselen en mechanismen voor toegangscontrole vast, met inbegrip van regelgebaseerde en rolgebaseerde beheersmaatregelen.

10.1.2 P7 Onboarding- en offboardingbeleid: Biedt procedurele stappen voor het initiëren en beëindigen van gebruikerstoegang in lijn met HR-acties.

10.1.3 P8 Beleid inzake informatiebeveiligingsbewustzijn en opleiding: Versterkt de verantwoordelijkheden van gebruikers voor accountbeveiliging en het beschermen van authenticatiemiddelen.

10.1.4 P13 Beleid inzake gegevensclassificatie en etikettering: Stuurt toegangsniveaus op basis van gegevensclassificatie en waarborgt dat grenzen aan rechten aansluiten op gevoeligheidsniveaus.

10.1.5 P22 Beleid inzake logging en monitoring: Waarborgt dat audittrails voor alle accountgerelateerde activiteiten worden verzameld en beoordeeld om afwijkingen of ongeautoriseerd gebruik te detecteren.

10.1.6 P30 Incidentresponsbeleid: Regelt escalatie, indamming en acties na incidenten in gevallen van misbruik van rechten of ongeautoriseerde accountactiviteit.

10.2 Deze beleidslijnen werken gezamenlijk om een samenhangend, risicogebaseerd kader voor identiteits- en toegangsbeheer binnen de organisatie af te dwingen.

**11. Referentienormen en -raamwerken**

11.1 Dit beleid is afgestemd op wereldwijd erkende normen voor cyberbeveiliging en regelgevende kaders die veilig beheer van identiteiten, toegang en rechten voorschrijven als kernonderdeel van de informatiebeveiliging van de organisatie.

**11.2 ISO/IEC 27001:**

11.2.1 Clausule 6.1.3 vereist dat organisaties risico's voor informatiebeveiliging bepalen, evalueren en behandelen, waarmee toegangs- en rechtenbeheer een formele, risicogebaseerde beheersmaatregel wordt die is ingebed in het ISMS-planningsproces.

11.2.2 Clausule 8.1 - Operationele planning en beheersing: versterkt de implementatie van technische en procedurele waarborgen die gebruikers- en geprivilegieerde toegang reguleren.

**11.3 ISO/IEC 27002:2022 - Beheersmaatregelen 5.15 tot en met 5.18:**

11.3.1 Beheersmaatregel 5.15 - beheer van gebruikerstoegang: ondersteunt formele processen voor toegangsverlening, autorisatie van toegang en periodieke beoordeling van toegangsrechten.

11.3.2 Beheersmaatregel 5.16 - identiteitsbeheer: stelt eisen aan unieke identiteiten, levenscyclusbeheer en het afdwingen van veilige authenticatie.

11.3.3 Beheersmaatregel 5.17 - authenticatie-informatie: waarborgt dat authenticatiemiddelen veilig worden beheerd en gebruikt gedurende de gehele levenscyclus van gebruikersaccounts.

11.3.4 Beheersmaatregel 5.18 - geprivilegieerde toegangsrechten: wordt volledig afgedekt via rolgebaseerde toewijzing van rechten, auditing en vereisten voor goedkeuring van verhoogde toegang.

11.4 Deze beheersmaatregelen sturen op een gestructureerde implementatie van accountregistratie, uitschrijving, scheiding van rechten en gebruik van authenticatie-informatie. Het beleid dwingt governance van de identiteitslevenscyclus, just-in-time-toegang en monitoring van verhoogde sessies af om ongeautoriseerd systeemgebruik te voorkomen.

**11.5 NIST SP 800-53 Rev.5:**

11.5.1 AC-1 (Beleid inzake toegangscontrole) en AC-2 (Accountbeheer): vertaald in beleidsvereisten voor toegangsgoedkeuringen, roltoewijzing en auditing van gebruikersaccounts.

11.5.2 AC-5 (functiescheiding (SoD)) en AC-6 (beginsel van minimale bevoegdheden): ingevuld via beperking van rechten, afstemming op functies en dubbele goedkeuring voor taken met een hoog risico.

11.5.3 IA-2 tot en met IA-5 (Identificatie en authenticatie): afgedwongen via sterke authenticatiemechanismen, regels voor de levenscyclus van authenticatiemiddelen en vereisten voor multifactorauthenticatie.

11.5.4 AU-2, AU-12 (auditlogging en analyse): afgedekt via sessieopname en monitoring van geprivilegieerde activiteiten in gevoelige omgevingen.

**11.6 AVG (Verordening (EU) 2016/679):**

11.6.1 Artikel 32 - Beveiliging van de verwerking: vereist toegangsbeheersmaatregelen en mechanismen voor identiteitsverificatie ter bescherming van persoonsgegevens. Hieraan wordt voldaan door accountgoedkeuringen, rechtenbeoordelingen en sterke authenticatiemaatregelen te verplichten.

11.6.2 Artikel 5(1)(f) - Integriteit en vertrouwelijkheid: waarborgt dat persoonsgegevens uitsluitend toegankelijk zijn voor geautoriseerde gebruikers met legitieme rollen, versterkt door handhaving van accountbeheer.

11.6.3 Overweging 39: verlangt duidelijke beperking van toegang en verantwoordingsplicht; dit beleid ondersteunt volledige herleidbaarheid van gebruikersidentiteiten en toewijzing van rechten.

**11.7 EU NIS2-richtlijn (2022/2555):**

11.7.1 Artikel 21(2)(a, d): vereist dat entiteiten beleid voor toegangsbeheer afdwingen en authenticatiemiddelen en geprivilegieerde sessies veilig behandelen, ondersteund door de beheersmaatregelen voor toegangsverlening, bewaking en uitzonderingen in dit beleid.

11.7.2 Artikel 21(3): bevordert discipline in toegang en sterke borging van identiteiten in kritieke sectoren; hieraan wordt voldaan door het gebruik van unieke identificatoren, RBAC en tijdgebonden verhoogde toegang.

**11.8 EU DORA (2022/2554):**

11.8.1 Artikel 5 - ICT-governance en beheersing: schrijft geformaliseerde processen voor ICT-gebruikersbeheer voor, afgedekt via gedocumenteerde toegangsverlening, deactivering en afhandeling van uitzonderingen.

11.8.2 Artikel 9 - ICT-risicomanagement: verplicht organisaties systemen te beveiligen door toegangsbeperkingen en bewaking, afgedekt via multifactorauthenticatie, logging van geprivilegieerde toegang en gecentraliseerde beoordelingen.

**11.9 COBIT 2019:**

11.9.1 DSS01 - Managed Operations: bevordert de handhaving van gestandaardiseerde operationele beheersmaatregelen, waaronder levenscyclusbeheer van gebruikersaccounts en documentatie van toegang.

11.9.2 DSS05 - Managed Security Services: weerspiegelt veilig beheer van gebruikers- en systeemrechten en ondersteunt risicobeperking via het beginsel van minimale bevoegdheden en validatie van audittrails.

11.9.3 APO13 - Managed Security: vereist toegangsgovernance over digitale activa en wordt ingevuld via geformaliseerde praktijken voor autorisatie van accounts en rollen met vereisten voor periodieke beoordeling.