| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Voer hier de naam van de geregistreerde rechtspersoon in | | | | | | | |
| Documentnummer:<br>P11S | | | | | Documenttitel:<br>**Beleid inzake beheer van gebruikersaccounts en privileges** | | | | | | | |
| 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 | Clausules 5.3, 8 | Rollen, verantwoordelijkheden en operationele planning en beheersing voor het beheer van gebruikerstoegang |
| ISO/IEC 27002:2022 | Beheersmaatregel 8 | Beheersmaatregelen voor toewijzing, beoordeling en verwijdering van verhoogde privileges |
| NIST SP 800-53 Rev.5 | AC-2, AC-5, AC-6 | Accountaanmaak, monitoring, minimale privileges en functiescheiding |
| EU NIS2 | Artikel 21(2)(d) | Beheer van gebruikerstoegang voor essentiële en belangrijke entiteiten |
| EU DORA | Artikel 9(2)(b) | Beheersing van geprivilegieerde toegang bij financiële entiteiten |
| COBIT 2019 | DSS05.03, DSS05.04 | Toegangsverlening, intrekking van toegangsrechten en periodieke beoordeling van gebruikerstoegang |
| AVG | Artikel 32 | Passende toegangsbeheersmaatregelen ter bescherming van persoonsgegevens |

## 1. Doel

1.1 Dit beleid stelt regels vast voor het beheer van gebruikersaccounts en toegangsrechten op een veilige, consistente en traceerbare wijze. Het waarborgt dat uitsluitend geautoriseerde gebruikers toegang hebben tot systemen en gegevens en dat die toegang passend is bij hun rol en verantwoordelijkheden.

1.2 Doeltreffend beheer van accounts en privileges is essentieel om ongeautoriseerde toegang te voorkomen, insiderdreigingen te beperken en naleving van ISO/IEC 27001, de AVG en andere toepasselijke wettelijke en regelgevende vereisten te waarborgen.

1.3 Dit beleid stelt de organisatie in staat eigenaarschap en verantwoordelijkheid voor accountgebruik toe te wijzen, privilege-escalaties te volgen en te auditen, en toegang veilig uit te schakelen of in te trekken wanneer deze niet langer nodig is.

1.4 Daarnaast beschermt het de bedrijfsvoering tegen operationele fouten of misbruik als gevolg van bovenmatige of onbeheerde toegang en helpt het het risico op onbedoelde datalekken, misbruik van privileges of niet-naleving van wet- en regelgeving te verminderen.

## 2. Reikwijdte

### 2.1 Dit beleid is van toepassing op:

2.1.1 alle werknemers, stagiairs, contractanten en gebruikers van derden met toegang tot de IT-systemen van de organisatie;

2.1.2 alle systemen, apparaten, diensten en platforms die door of namens de organisatie worden beheerd, met inbegrip van cloudplatforms, on-premise-infrastructuur en tools van derden.

**2.2 Het beleid heeft betrekking op alle typen gebruikersaccounts, waaronder:**

2.2.1 persoonlijke gebruikersaccounts op naam, zoals e-mailaccounts en systeemaanmeldingen;

2.2.2 beheerdersaccounts en systeemaccounts;

2.2.3 tijdelijke accounts, gastaccounts of toegangsaccounts voor derden;

2.2.4 serviceaccounts die worden gebruikt door toepassingen of automatiseringssystemen.

2.3 Dit beleid is van toepassing op de volledige accountlevenscyclus: van aanmaak en goedkeuring tot wijziging, monitoring en deactivering. Dit omvat initiële toegangsverlening tijdens onboarding, beoordelingen van toegangsrechten bij rolwijzigingen en intrekking van toegangsrechten tijdens offboarding.

**3. Doelstellingen**

3.1 Alle systeemgebruikers moeten beschikken over unieke, traceerbare gebruikersidentiteiten, zodat verantwoording is gewaarborgd en het gebruik van gedeelde inloggegevens wordt uitgesloten.

3.2 Het beginsel van minimale bevoegdheden moet worden afgedwongen, zodat gebruikers uitsluitend het minimale toegangsniveau krijgen dat nodig is om hun werkzaamheden uit te voeren.

3.3 Ongeautoriseerde toegang tot gevoelige systemen of gegevens moet worden voorkomen door middel van duidelijk gedocumenteerde goedkeurings- en beoordelingsprocessen.

3.4 Gebruikersaccounts moeten tijdig worden gedeactiveerd wanneer deze niet langer nodig zijn, bijvoorbeeld bij uitdiensttreding, afloop van een contract of rolwijzigingen.

3.5 Een veilige en auditwaardige omgeving moet in stand worden gehouden door alle accountwijzigingen, goedkeuringen en periodieke beoordelingen te documenteren.

3.6 Privilegeverhoging moet strikt worden beheerst, onafhankelijk worden goedgekeurd en worden gelogd, en verhoogde toegang moet onverwijld worden ingetrokken wanneer deze niet langer nodig is.

**4. Rollen en verantwoordelijkheden**

**4.1 Algemeen directeur (GM)**

4.1.1 Draagt de eindverantwoordelijkheid voor de handhaving van dit beleid.

4.1.2 Waarborgt dat accountbeheer in lijn is met de certificeringseisen van ISO/IEC 27001 en relevante wettelijke verplichtingen, zoals de AVG.

4.1.3 Moet onmiddellijk worden geïnformeerd over iedere ongeautoriseerde toegang, ieder beveiligingsincident of iedere beleidsovertreding met betrekking tot gebruikersaccounts.

4.1.4 Houdt toezicht op beleidsevaluaties, audits en handhavingsmaatregelen.

**4.2 IT-manager of externe IT-dienstverlener**

4.2.1 Is verantwoordelijk voor de technische implementatie van maatregelen voor account- en privilegebeheer binnen de systemen die door de organisatie worden gebruikt.

4.2.2 Mag gebruikersaccounts uitsluitend aanmaken, wijzigen en deactiveren op basis van gedocumenteerde goedkeuringen.

4.2.3 Moet wachtwoordcomplexiteit, schermvergrendeling na een time-out, multifactorauthenticatie (indien beschikbaar) en systeemlogging afdwingen.

4.2.4 Moet beveiligde registraties bijhouden van alle toegangsgoedkeuringen, accounteigenaarschap, privilege-escalaties en intrekkingen van toegangsrechten.

4.2.5 Moet toezien op ongeautoriseerde of verweesde accounts en afwijkingen rapporteren 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 actualisering**

**9.1 Dit beleid moet ten minste jaarlijks door de GM en de IT-manager worden beoordeeld om naleving te waarborgen van:**

9.1.1 de actuele beheersmaatregelen en richtlijnen van ISO/IEC 27001:2022;

9.1.2 actualisaties in wet- en regelgeving, zoals de AVG, DORA en NIS2;

9.1.3 wijzigingen in systemen, diensten of de bedrijfsstructuur.

**9.2 Beoordelingen moeten ook worden uitgevoerd na:**

9.2.1 significante beveiligingsincidenten of auditbevindingen;

9.2.2 ingrijpende wijzigingen in IT-systemen of accountarchitectuur;

9.2.3 de invoering van nieuwe platforms waarvoor integratie van toegangscontrole vereist is.

9.3 Alle wijzigingen moeten worden goedgekeurd door de GM en duidelijk worden gecommuniceerd aan de betrokken medewerkers.

**10. Gerelateerd beleid en samenhang**

10.1 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: stelt verantwoording en beslissingsbevoegdheid vast voor toegangsgoedkeuringen en toezicht.

10.2 P4S – Beleid inzake toegangscontrole: regelt de organisatiebrede afdwinging van toegangscontrole en authenticatiemethoden.

10.3 P7S – Onboarding- en offboardingbeleid: waarborgt dat accountaanmaak en verwijdering zijn ingebed in door HR beheerde personeelswijzigingen.

10.4 P8S – Beleid inzake bewustwording en opleiding op het gebied van informatiebeveiliging: traint gebruikers in veilige accountpraktijken en verwachtingen ten aanzien van gebruik.

10.5 P30S – Incidentresponsbeleid (P30): definieert de te nemen maatregelen als accountmisbruik leidt tot een beveiligingsincident of ongeautoriseerde openbaarmaking.

**11. Referentienormen en -raamwerken**

**11.1 ISO/IEC 27001**

11.1.1 Clausule 5.3: vereist dat rollen en verantwoordelijkheden voor informatiebeveiliging duidelijk worden toegewezen en afgedwongen.

11.1.2 Clausule 8.1: vereist dat operationele planning en beheersing ook het beheer van gebruikerstoegang omvatten.

**11.2 ISO/IEC 27002**

11.2.1 Beheersmaatregel 8.2: beschrijft technische en procedurele beheersmaatregelen voor het toewijzen, beoordelen en verwijderen van verhoogde privileges.

**11.3 NIST SP 800-53 Rev.5**

11.3.1 AC-2: vereist accountaanmaak, monitoring en intrekking van toegangsrechten op basis van vastgestelde rollen en processen.

11.3.2 AC-5: behandelt functiescheiding om conflicten of misbruik van privileges te voorkomen.

11.3.3 AC-6: schrijft toepassing van het beginsel van minimale privileges voor op alle toegangsrechten.

**11.4 AVG**

11.4.1 Artikel 32: vereist passende toegangsbeheersmaatregelen om persoonsgegevens te beschermen tegen ongeautoriseerde toegang of wijziging.

**11.5 EU NIS**

11.5.1 Artikel 21(2)(d): schrijft beheer van gebruikerstoegang voor als onderdeel van kernbeheersmaatregelen voor essentiële en belangrijke entiteiten.

**11.6 EU DORA**

11.6.1 Artikel 9(2)(b): vereist dat financiële entiteiten toegangsbeheersmaatregelen implementeren die geprivilegieerde rechten beperken en bewaken.

**11.7 COBIT 2019**

11.7.1 DSS05.03: specificeert toegangsverlening en intrekking van toegangsrechten als onderdeel van IT-governance.

11.7.2 DSS05.04: verlangt doorlopende beoordeling en afstemming van gebruikerstoegang op organisatierollen.