ProRail

Bijlage 1.4 ProRail Toegangsbeleid uit IBB2.4

Hieronder een deel van het toegangsbeleid wat door ProRail gehanteerd wordt. Het is het relevante deel wat van toepassing is bij de aanbesteding van de SaaS dienst personeelsplanningsysteem.

1 Soorten accounts

Principieel is dat iedereen op persoonlijke titel en met een persoonlijk account aanmeldt en authentiseert op de ProRail infrastructuur.
Uitzondering wordt gemaakt voor systeemaccounts en voor die situaties waar persoonlijk inloggen technisch nog niet mogelijk is (tijdelijke ontheffing).

1.1 Persoonlijk Account

Een persoonlijk account vertegenwoordigt één “identiteit” binnen ProRail.
Dit account kent een aantal categorieën:

Categorie	Bron:	Opmerking:
Eigen personeel	SAP-HR	
Inhuur personeel “op naam”	SAP-HR + Inhuurdesk	
Inhuur personeel “op capaciteit”	AKI projectnummer + IdM	(=projectaccount)
Extern Account *)	CRm / AM registratie	Format: EX_bedrijf_naam
Persoonlijk account via Federatie	Gefedereerde partij	

*) Een extern Account krijgt toegang tot een specifieke applicatie of zone.

- Een specifieke directory in SharePoint (Ook online) voor samenwerking
- Een specifieke applicatie, zoals SAP.

Externe accounts worden, na 180 dagen niet gebruikt te zijn, verwijderd.
Accounts bij Inhuur op capaciteit hebben een looptijd van maximaal 180 dagen en kunnen verlengd worden, als dat gewenst is, met max. 180 dagen, tot einde contract.
Bij einde dienstverband of einde registratietermijn worden de accounts geblokkeerd en zijn niet overdraagbaar aan anderen.
Aanmelden met een andermans identiteit is niet toegestaan.

1.2 Beheer-account (persoonlijk)

Speciaal account om technisch beheer te doen op de Systemen en binnen domeinen met extra rechten. Deze accounts zijn herkenbaar als beheeraccount (voorvoegsel BEH-) en zijn altijd persoonlijk. Activiteiten uitgevoerd met dit account dient te worden gelogd.
Aanmelden met een andermans identiteit is niet toegestaan.
Dit account mag niet voor KA taken gebruikt worden, dus naast dit account heeft een gebruiker ook een normaal account.

1.3 Groepsaccount / Functioneel account

Een groepsaccount is in het leven geroepen voor generiek gebruik van een bepaalde omgeving en mag alleen ingezet worden bij een applicatie/systeem classificatie met ten hoogste BIV=LLL of binnen een beschermde omgeving zoals een VL-Post of OCCR.
Een groepsaccount mag dus niet worden gebruikt voor toegang waar 2-factorauthenticatie vereist is. (er worden op groepsaccounts geen Tokens of smartcards uitgegeven).
Om veiligheidsreden wordt het gebruik van groepsaccounts slecht bij dringende noodzaak toegestaan en pas na een gedegen risicoanalyse.
Groepsaccounts van ProRail worden alleen Intern gebruikt (ook geen federatie).
Voor Office365 wordt een tijdelijke “alleen-lezen” toegang toegestaan voor KA-groepsaccounts gedurende de migratie naar Office365, mits vertrouwelijkheid van de inhoud laag is (Intern).
Per account moet een motivatie en een migratieplan naar Persoonlijke accounts overlegd worden.

1.3.1 Groepsaccount Receptie/Beveiliging

Er zijn speciale functies die op capaciteit gecontracteerd zijn (bijvoorbeeld receptie).
Hier kan per dagdeel een andere medewerker zitten maar de inhoud is gericht op de functie.
Functies: onder het account: Exchange (E-Mail, Agenda). SSP, SP365, Specifieke toepassingen voor de functie (Toegangscontrole, bezoekersregistratie e.d.).

Limiteringen.

- Geen toegang tot toepassingen als LMS, e.d.
- Één account per functie/locatie. Bijvoorbeeld:
  1x receptie Inktpot, 1x receptie Tulpenburgh ….

1.4 Monitoraccount / Kiosk Account

Monitor accounts en Kiosk accounts ondersteunen slechts één applicatie.

- **Kiosk accounts** kunnen alleen een browser opstarten en zijn afgeschermd van de rest van de interne infrastructuur.
  Het is niet toegestaan op dit accounts een andere toepassing beschikbaar te stellen.
- **Monitor Accounts** kunnen alleen de monitor-applicatie opstarten en mag alleen in de beschermde omgeving van de VL post en OCCR gebruikt worden omdat de beschermingsmaatregel “Schermbeveiliging” is uitgeschakeld
  Het is niet toegestaan op dit account andere toepassingen beschikbaar te stellen.
  Onder strikte voorwaarden en aangetoonde noodzaak, kan ontheffing verleend worden voor “alleen-lezen” toegang op een beperkt deel van de SP365 bibliotheek.

1.5 Groepsmailbox / Functionele mailbox

Een groepsmailbox is een mailbox voor gezamenlijk gebruik van een groep of afdeling.
Hier kan een Postbus en/of een of meer groepsagenda’s in zitten.
De mailbox komt doorgaans onder beheer en op naam van de aanvrager.
Als het technisch noodzakelijk is om hiervoor een (AD-) account aan te maken, wordt het gebruikersnaam en Wachtwoord hiervan niet vrijgegeven en is de inlogmogelijkheidgeblokkeerd.

1.6 Werkplekaccount

Werkplekken die alleen een minimale configuratie hebben en alleen als drager van een (gevirtualiseerde) applicatie met een eigen autorisatie en authenticatie mechanisme (OCCR werkplekken) kan optreden, kunnen een accountnaam hebben met de naam van de werkplek. Deze werkplekken bevinden zich in een beschermde omgeving met een zwaarder fysiek toegangsregime (zoals bv. een VL post). In deze situatie is wachtwoord-loze toegang toegestaan.

1.7 Systeemaccount

Speciaal account om systemen en databases technisch te ontsluiten.
Deze mogen dus uitsluitend voor die functie gebruikt worden.
Werken lokaal op één server.
Deze accounts worden zodanig geconfigureerd dat het nooit mogelijk is om er op een normale werkplek mee in te loggen.
Wachtwoorden van deze accounts worden niet afgegeven.

1.7.1 Systeemaccount Azure/SP365/CRM365

Dit is een verbijzondering van het “normale” systeemaccount.
Standaard worden deze accounts in de lokale AD aangemaakt en gesynchroniseerd.
In uitzonderlijke gevallen, dit ter beoordeling van CISO, kan een uitzondering gemaakt worden voor On-line Only routines. Deze beperkte set van zg. OnMicrosoft accounts valt onder beheer van ECM beheer.

1.8 Installatie account

Dit installatieaccount is bedoeld om vanuit het oogpunt “Running the Business” autodeployment van nieuwe softwareversies te kunnen uitvoeren. Het account is standaard *disabled* en kan dus alleen doormiddel van een change geactiveerd worden om voor een bepaalde tijd, 1-2 dagen, gebruik te kunnen maken van dit account om software uit te rollen (autodeployment), hierna zal het account weer worden disabled.
Deze accounts worden zodanig geconfigureerd dat het nooit mogelijk is om er op een normale werkplek mee in te loggen.
Wachtwoorden van deze accounts worden indien noodzakelijk afgegeven maar na gebruik vervangen.

1.9 Local-Admin / Root-account

Speciaal account om technisch beheer te doen op een bepaald systeem met doorgaans extra rechten.
Is geen gebruikersnaam, persoonsnaam of bedrijfsnaam.

1.10 Overige Accounts

Er zijn speciale systemen, zoals b.v. de INTTEL, waar geen specifieke policy op te implementeren is.
Voor deze systemen geldt een risico-afweging en een set van maatregelen “op maat”

2 Wachtwoordbeleid

In de werkinstructies op uitvoerend niveau is het beleid verder uitgewerkt.
Voor bepaalde domeinen kunnen aangepaste regels gelden.

2.1 **Algemene policies** (Minimum voor alle zones en applicaties)**:**

Type wachtwoord-eis	Algemene-invulling
Wachtwoord lengte	Minimaal **8** karakters/tekens
Password geldigheid	90 dagen
Wachtwoord historie	24
Wachtwoord verloopt	1 dag (mogelijkheid om na expiratie te wijzigen)
Herinnering Wachtwoord verloopt	Dag 76 en 88
Wachtwoord complexiteit	• Mag geen gebruikersnaam zijn, of delen (3 of meer opeenvolgende karakters) van de volledige naam. • Bevat karakters/tekens uit 3 van de 4 onderstaande categorieën: ➢ Hoofdletters (A…Z) ➢ Kleine letters (a … z) ➢ Cijfers (0 … 9) ➢ Vreemde tekens (bijv. !$#%)
Repeterend patroon	Restrictie aanbrengen vwb tegen gaan logische opvolging is niet vereist.
Account lockout	Na 5 maal fout inloggen (verkeerd wachtwoord) wordt het desbetreffende account geblokkeerd.

2.2 Afwijking per accountsoort

2.2.1 **Persoonlijk Account**

➢ Geen afwijkingen

2.2.2 **Beheer Account**

➢ Geen afwijkingen

2.2.3 **Groepsaccount / Functioneel account**

➢ Standaard geen afwijkingen

In uitzonderlijke gevallen, in een beschermde omgeving, kan door de security manager, na risicoanalyse, een uitzondering worden toegestaan.

2.2.4 **Monitor Account / Kiosk Account**

Zowel Monitor account als Kiosk Account hebben door hun specifieke plaats een één-applicatie functie geen Schermbeveiliging en geen wachtwoord.

2.2.5 **Groepsmailbox / Functionele mailbox**

➢ Heeft geen inlogmogelijkheid.

2.2.6 **Werkplekaccount**

➢ Algemene policies bij aanwezigheid van een wachtwoord.

2.2.7 **Systeemaccount**

➢ Heeft geen Inlogmogelijkheid, op een werkplek.

Dit wachtwoord moet complex, ten minste een lengte van 15 posities en 3 karaktersoorten, zijn.

2.2.8 **Installatie account**

➢ Heeft geen Inlogmogelijkheid, op een werkplek.

Dit wachtwoord moet complex, ten minste een lengte van 15 posities en 3 karaktersoorten, zijn.

2.2.9 Local-Admin / Root-account

- De security policy wbt lokale admin/root-wachtwoorden heeft wat afwijkingen:

Alle ProRail domeinen			
Servers	***Alle platformen***	***Clients***	***Alle platformen***
Installatie (inrichting-basis)		Installatie (inrichting-basis)	
Uniek wachtwoord?	**Nee**	Uniek wachtwoord?	**Nee**
Sterk wachtwoord?	Ja	Sterk wachtwoord?	Ja
Password never expires	**Ja**	Password never expires	**Ja**
Implementatie (uitrol)		Implementatie (uitrol)	
Gedeeld alg. wachtwoord?	Nee	Uniek wachtwoord?	**Nee**
Sterk wachtwoord?	Ja	Sterk wachtwoord?	Ja
Password never expires	**Ja**	Password never expires	**Ja**

2.2.10 Overige accounts

- Invulling a.d.v. risico's en mogelijkheden "op maat" in lijn met de risico-hoogte..

2.3 Opslag van wachtwoorden

Principieel dienen wachtwoorden niet geregistreerd te zijn. Een wachtwoord is iets persoonlijks wat iedereen, net als de pincode, dient te onthouden.

2.3.1 Uitzonderingen

Op de bovenstaande regel zijn een aantal, vrijwel onvermijdbare, uitzonderingen te bedenken. Te denken valt dan aan:

- Wachtwoorden binnen een testomgeving.
- Wachtwoorden van databases
- Wachtwoorden van systeemaccounts
- Enz..

Voor deze groepen kan een veilige, beperkt toegankelijke opslagomgeving gemaakt worden. (Password Vault oid.)
Note: Bij ICT-Opeatie is hiervoor het product Keepass in gebruik.

2.3.2 Eisen aan de opslag

- Toegang is gebonden aan gebruikersgroepen waarbij alleen de rechthebbenden op basis van persoonlijke Identiteit, gelogd, toegang hebben tot de eigen set van wachtwoorden.
- Opslag is beveiligd met een veilige encryptie (AES e.d.)
- Opslagmechanisme is universeel toepasbaar binnen ProRail en wordt dus als standaard pakket aangeboden.