

Documenthistorie (recent naar oud)

- 3 mrt 2020 [REDACTED] document geactualiseerd en tekstuele aanpassingen gedaan (o.a. RAV → AGM)
- 21 feb. 2019 [REDACTED] "BIG" vervangen door "BIO". Beleidsvoornemen 2fA verwijderd, omdat dit document staand beleid beschrijft, geen beleidsvoornemens.
- 20 feb. 2019 [REDACTED] verduidelijkt – na overleg met [REDACTED] - dat local admin accounts voor functioneel beheerders separate en persoonlijke accounts zijn.
- 15 jan 2019 [REDACTED] het gebruik van local administrator accounts aangescherpt.
- 8 jan 2019 [REDACTED] geen standaard initieel wachtwoord meer, maar willekeurig gekozen. Verificatiescript bij aanvraag nieuw wachtwoord vermeld.
- 18 dec .2018 [REDACTED]: verwijzing naar Wet bescherming persoonsgegevens weggehaald, omdat verwijzing naar AVG volstaat.
- 17 dec. 2018 [REDACTED] paragraaf over x-accounts (accounts voor leveranciers) toegevoegd.
- 31 okt. 2018 [REDACTED]: regel inzake default accounts toegevoegd.
- 17 mei 2018 [REDACTED]: beleid inzake door- en uitstroom in afzonderlijke paragraaf gezet.
- 7 mei 2018 [REDACTED] toegevoegd: paragraaf over patchkasten.
- 25 apr. 2018 [REDACTED]: toegevoegd: extra informatie over regels voor samenstelling account; onderscheid van meerdere typen accounts naar aanleiding van invoering t-accounts; stukje over niet-persoonsgebonden accounts; stukje over beleid *fysieke* toegang leveranciers.
- 14 mrt 2018: [REDACTED] toegevoegd "Wanneer een wachtwoord bijna verloopt, ontvangt de gebruiker een systeembericht, waarin het wachtwoordbeleid wordt meegedeeld."
- 7 mrt 2018: [REDACTED]: voorbeeldaccountnaam gepseudonimiseerd op verzoek van [REDACTED]
- 6 mrt 2018. [REDACTED] nadere beschrijving van de accounts met speciale beheerdersrechten toegevoegd. De informatie komt van [REDACTED].
- 6 mrt. 2018. [REDACTED]: opmerking dd. 5 januari van service manager Remco Aarts verwerkt, betreffend de brongegevens voor de profielen, en vraag beantwoord. **Thans heeft dit document een formele status.**
- 16 jan. 2018. [REDACTED]: stukje over accounts uitgebreid met naamgeving accounts en onderscheid gebruikers- versus beheerdersaccount.
[REDACTED] beoordeelt document en plaatst opmerking en vraag.
- 4 jan. 2018. [REDACTED] feedback van facility-medewerker [REDACTED] aangaande fysieke beveiliging verwerkt.
- 2017 [REDACTED] aanmaak op 2 maart 2017 en in dit jaar diverse wijzigingen. Doel: voldoen aan NEN7510 en BIG.

Inhoud

Inleiding	3
Fysieke toegang	3
Beleid	3
Medewerkers	3
Leveranciers	3
Patchkasten.....	3
Operationele uitwerking	3
Logische toegang	4
Rechten.....	4
Accounts	4
Niet-persoonsgebonden accounts	5
Wachtwoorden/-zinnen	6
Verstrekking van een wachtwoord	6
Implementatie wachtwoordbeleid	6

Toegang tot de applicatie.....	7
Door- en uitstroom van een medewerker	7
Controle inzake logische toegang.....	7

Inleiding

Dit document bevat het beveiligingsbeleid van VGGM inzake de fysieke en de logische toegang tot informatiesystemen. Het is ondergeschikt aan het Informatiebeveiligingsbeleid van VGGM en een uitwerking hiervan ten aanzien van de toegang tot gegevens, de middelen om gegevens te verwerken en de fysieke ruimten die gegevens of middelen bevatten. Het bevat tevens de uitwerking in middelen en regels voor het proces *Operationeel beheer*.

Fysieke toegang

Beleid

Medewerkers

Functioneel. Een medewerker heeft alleen toegang tot de ruimten die hij voor zijn functie of rol moet gebruiken.

Profiel. De toegang tot ruimten die voorzien zijn van een paslezer wordt toegekend op grond van profielen. Een profiel bevat de toegangsrechten. De profielen staan uitgewerkt in het digitale beheersysteem voor fysieke toegang. De brongegevens van de medewerkers, bijvoorbeeld de afdeling waar het profiel aan gekoppeld is, staan in het personeelsinformatiesysteem.

Zo krijgt een beroepsbrandweerman toegang op grond van het profiel *Beroepsbrandweer* dat hem is toegekend. Hierbij wordt nog weer onderscheid gemaakt in functie en werklocatie.

Logging. Handelingen met betrekking tot de toegang of het (technisch) regelen van de toegangsrechten worden gelogd.

Tag. Een tag, die toegang geeft tot gebouwen en ruimten, wordt op naam verstrekt en is persoonsgebonden. Aan gasten worden geen tags verstrekt. Zij worden opgehaald bij de receptie en begeleid in het pand.

Bij uitdiensttreding wordt de tag van de medewerker zo spoedig mogelijk geblokkeerd.

Leveranciers

Medewerkers van het schoonmaakbedrijf hebben een toegangspas op hun eigen naam gesteld. Overige leveranciers hebben een toegangspas op hun bedrijfsnaam gesteld.

Patchkasten

Patchkasten of de ruimten waarin zij staan zijn afgesloten en alleen toegankelijk voor bevoegd personeel met een paslezer of sleutel.

Operationele uitwerking

[Redacted content]

- [Redacted]

Logische toegang

Rechten

[Redacted]

[Redacted] voert vervolgens de technische wijziging door. Zonder opdracht, toestemming [Redacted].

Beheerdersrechten. De technisch beheerders hebben niet meer rechten dan zij voor hun dagelijks werk nodig hebben. Zij hebben standaard geen recht om in de homedirectories van collega's te komen. Zij mogen daarin alleen komen na toestemming van de betrokkene; of op last van een leidinggevende, mits dit juridisch is toegestaan. Wanneer het recht van een technisch beheerder wordt uitgebreid tot toegang tot een homedirectory, dan wordt dit met opgaaf van de reden geregistreerd in het meldingenbeheersysteem Topdesk.

Accounts

[Redacted]

Bij indiensttreding ontvangt een medewerker een papieren welkomstbrief met daarin zijn unieke gebruikersnaam en standaard wachtwoord. Dit wachtwoord moet hij veranderen bij de eerste keer inloggen.

Gebruikersnaam. [Redacted]

[Redacted]

Accounttypen. [Redacted]

[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

A-accounts.

[REDACTED]

Het gebruik van local administrator accounts.

[REDACTED]

Niet-persoonsgebonden accounts

Naast de bovengenoemde typen persoonsgebonden account zijn er drie categorieën niet-persoonsgebonden accounts:

1. systeemtechnische accounts
2. groepsaccounts
3. x-accounts voor externen die geen ketenpartner zijn: leveranciers

Systeemtechnische accounts.

[REDACTED]

Groepsaccounts.

[REDACTED]

[Redacted text block]

De redenen om groepsaccounts in te voeren is efficiëntie: besparing van licentiekosten en parate beschikbaarheid van een account.

[Redacted text block]

[Redacted text block]

Wachtwoorden/-zinnen

Het beleid van VGGM inzake wachtwoorden van gebruikers voor toegang tot ons netwerk houdt het volgende in:

[Redacted text block]

[Redacted text block]

Verstrekking van een wachtwoord

[Redacted text block]

[Redacted text block]

Implementatie wachtwoordbeleid

[Redacted text block]

[Redacted text block]

¹ Deze eis kan in Windows worden ingesteld zonder dat het nodig is een wachtwoordfilter te programmeren. [Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

Toegang tot de applicatie

Opstarten van de applicatie. De mogelijkheid een applicatie op te starten wordt bepaald door het lidmaatschap van de desbetreffende groep gebruikers.

Inloggen en werken in de applicatie. Sommige applicatie vereisen een afzonderlijke inlog. De toegang tot binnen de applicatie (inloggen in de applicatie) en de verwerkingsmogelijkheden binnen een applicatie worden in de applicatie geregeld door de functioneel beheerder. Het afdelingshoofd is verantwoordelijk voor de formele toekenning, de functioneel beheerder verantwoordelijk voor de toekenning binnen de applicatie overeenkomstig de opdracht van de leidinggevende.

Door- en uitstroom van een medewerker

Doorstroom. [Redacted text block]

Uitstroom. [Redacted text block]

Controle inzake logische toegang

[Redacted text block]