

Wachtwoordenbeleid voor OT-systemen

Eisen aan wachtwoorden voor
operationele technologie
(bedienings- en
bewakingssystemen)

Versie: 1.1

Vertrouwelijkheidsniveau:

Bedrijfsvertrouwelijk

Colofon

Versiebeheer en status

29 september 2022, Versie 1.1, In dit document is het recente wachtwoordenbeleid van GVB/ICT, waar van toepassing, overgenomen en aangevuld met het wachtwoordenbeleid uit de CSIR 2.4 van Rijkswaterstaat, Wim van Asperen, Cybersecurity Officer OT.

Contactpersoon Cybersecurity-officer OT, Wim van Asperen
Doorkiesnummer 0621854536
Faxnummer

Inhoudsopgave

1	Wachtwoorden voor OT.....	4
----------	----------------------------------	----------

1 Wachtwoorden voor OT

- 1.1. Indien - vanwege technische redenen - geen invulling gegeven kan worden aan het wachtwoordenbeleid hieronder, dan mag een alternatieve oplossing alleen na expliciete goedkeuring door de cybersecurity-office van GVB worden gerealiseerd en geïmplementeerd.
- 1.2. Indien er – tegen het beleid van GVB in - gebruik wordt gemaakt van ‘shared beheeraccounts’ dan dient het wachtwoord van een ‘shared’ account onmiddellijk na vertrek van een beheerder (leaver), maar uiterlijk binnen 2 dagen, vervangen te worden.
- 1.3. Opdrachtnemer zorgt ervoor dat wachtwoorden van alle accounts, zowel beheer als gebruikers, worden opgeslagen met een veilig one-way-hash mechanisme (SHA-2 of SHA-3) met een “salt” toevoeging.
- 1.4. Voor OT-systemen worden verschillende accounts onderkend, met elk hun eigen vereisten voor wachtwoordgebruik. N.B. Deze eisen zijn overgenomen van de CSIRT versie 2.4 van Rijkswaterstaat.
 - a. Standaardaccount fabrikant: Standaard accounts en -wachtwoorden die toegepast worden in OT-systemen van fabrikanten mogen niet worden gebruikt en dienen te zijn uitgeschakeld c.q. te zijn overschreven met een eigen sterk wachtwoord.
 - b. Gebruikers/Operatoraccount. Een persoonlijk account dat wordt gebruikt voor de bediening van OT systemen. Soort: persoonsgebonden (terug te herleiden naar een individu). Wachtwoord vervanging: 180 dagen. Wachtwoordlengte: minimaal 15 karakters. Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.
 - c. OT-applicatiebeheeraccount. Een persoonlijk account dat wordt gebruikt om de applicaties op het OT systeem te beheren. Soort: persoonsgebonden (terug te herleiden naar een individu). Wachtwoord vervanging: 180 dagen. Wachtwoordlengte: minimaal 15 karakters. Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.
 - d. OT-Systeemaccount (service/applicatie account). Een account dat ervoor zorg draagt dat een applicatie zonder menselijke interventie applicatieopdrachten kan uitvoeren onder speciale rechten. Soort: service. Wachtwoord vervanging: 365 dagen. Wachtwoordlengte: minimaal 20 karakters. Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.
 - e. OT-Administratoraccount. Een persoonlijk account dat op de systemen volledig beheer heeft d.m.v. administrator rechten. Soort: persoonsgebonden (terug te herleiden naar een individu). Wachtwoord vervanging: 180 dagen. Wachtwoordlengte: minimaal 20 karakters. Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.
- 1.5. Als het wijzigen van wachtwoorden niet automatisch kan worden afgedwongen, dient men te zorgen dat het procedureel wordt afgedwongen en geborgd.
- 1.6. Indien een wachtwoord fysiek moet worden opgeslagen (bijvoorbeeld, omdat dat volgens een veiligheidsprocedure moet), sla het wachtwoord dan op in een fysieke kluis. Zorg er dan voor dat de sleutel niet eenvoudig te vinden is of dat de kluis op een andere locatie staat.
- 1.7. De volgende zaken dienen niet te worden opgenomen in, of onderdeel uit te maken van, wachtwoorden:

- a. Namen van familieleden, huisdieren, vrienden, collega's, stripfiguren, etc.;
- b. Computernamen en -termen, commando's, naam van de software of hardware, naam van het bedrijf dat het heeft geleverd;
- c. Woorden verwijzend naar organisatie, object of locatie, bijvoorbeeld: GVB, Amsterdam, etc
- d. Geboortedata en andere persoonlijke informatie als adres en telefoonnummers;
- e. Eén van de voorafgaande woordsoorten, gevolgd door een getal (bijvoorbeeld: geheim01, welkom123, GuustFlater13, etc.).