

Wachtwoordbeleid

Toegangsbeveiligingsbeleid en voorschrift gebruikerswachtwoorden 2020-2021

Doelstelling

De doelstelling van dit document richt zich op een goed, begrepen en zo veel mogelijk afgedwongen beleid: Gebruikers dienen goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden in computersystemen en mobiele apparaten.

Voor het wachtwoordbeleid volgt Zadkine en haar onderdelen het [recente advies van het Nationaal Cyber Security Centrum \(NCSC\)](#) van het ministerie van Justitie en Veiligheid, om deze niet meer verplicht periodiek te laten wijzigen door de gebruiker. Dit verkleint de kans op eenvoudig te raden wachtwoorden en/of het opschrijven van wachtwoorden in verband met het mogelijk vergeten ervan.

Uitgangspunten

Gedragsregels hoe om te gaan met (het beheer van) wachtwoorden:

- Medewerkers en studenten worden op de hoogte gesteld van het informatieveiligheidsbeleid, regels- en richtlijnen. Het wachtwoordbeleid is hier onderdeel van en geldt voor alle systemen met wachtwoord beveiliging die op de instelling worden gebruikt
- Het beheer van gebruikerswachtwoorden wordt gedaan door middel van een formeel proces
- Gebruikerswachtwoorden zijn strikt persoonlijk, geheim en alleen bekend bij de gebruiker. Ze mogen niet met andere personen worden gedeeld of onveilig bewaard:
 - niet op papier vastleggen, tenzij in goed afgesloten meubilair / kluis
 - niet in onbeschermd vorm opslaan op computersystemen (een goede wachtwoordkluis/passwordmanager is wel toegestaan)
- Een initieel afgegeven wachtwoord moet zo snel mogelijk, in ieder geval binnen twee dagen worden gewijzigd
- Gebruik unieke wachtwoorden: wachtwoorden voor school mogen niet ook voor privé- of systemen/toepassingen van andere instellingen worden gebruikt

Kenmerken

Minimumlengte wachtwoord

- De gebruiker wordt aangemoedigd om een wachtzin in plaats van een wachtwoord te gebruiken; de minimumlengte is daarom vastgesteld op 13 tekens.
Makkelijker te onthouden, moeilijker te kraken door *'brute force'*

Complexiteit van het wachtwoord

- Tenminste 1 van de vereiste 13 tekens moet een speciaal karakter zijn (teken dat geen cijfer of letter is)
- De gebruiker krijgt een duidelijke handreiking voor de samenstelling van een veilige, niet te eenvoudig te raden of d.m.v. *'woordenboekaanval'* te kraken wachtwoord of -zin:
Deze bevat in ieder geval de volgende eisen:
 - mag niet gebaseerd zijn op iets dat iemand anders gemakkelijk zou kunnen raden of verkrijgen (zoals geboortedatum, naam familielid of andere eenvoudig te verkrijgen informatie)
 - Mag niet meerdere opeenvolgende gelijke tekens of voorspelbare reeksen bevatten en niet uitsluitend uit numerieke of alfabetische tekens
 - Mag niet enkel veel voorkomende woorden en/of namen bevatten (zoals W@chtwoord1234, Feyenoord1!!!, etc.)

Deze toelichting maakt deel uit van de procedure wijzigen wachtwoord.

Minimum geldigheid wachtwoord

- De wachtzin kent in tijd geen minimumgeldigheid en kan te allen tijde worden gewijzigd.
Het dient direct opnieuw ingesteld te worden wanneer (potentieel) misbruik wordt vermoed.

Maximum geldigheid wachtwoord

- Een wachtwoord is onbeperkt geldig en dient alleen opnieuw ingesteld te worden wanneer (potentieel) misbruik wordt vermoed.

Wachtwoord historie

- Er gelden geen beperkingen ten aanzien van wachtwoordhistorie.

Aanvulling voor mobiele apparaten

- Mobiele devices zoals smartphones/tablets dienen te worden afgeschermd middels een schermbeveiliging die minimaal moet worden ontgrendeld met minimaal een viercijferige (PIN) code en/of een biometrische beveiliging.
- Niet toegestaan zijn zogenaamde Swipe-beveiligingen (Niet veilig).
- De schermbeveiliging dient automatisch geactiveerd te worden na 60 seconden.

Aanvulling voor beheerders

Voor medewerkers van Zadkine met uitgebreide rechten met als doel het onderhouden van computersystemen (administrators rechten) zijn aanvullende voorwaarden.

- alle eisen zoals hiervoor gesteld zijn van toepassing, met als aanvulling:
- Gebruik van Multi Factor Authentication (MFA) bij alle systemen waarbij dit technisch mogelijk is
- Medewerker onderhoudt een overzicht van alle computersystemen waar hij/zij toegang tot heeft met administrators rechten.
- Standaardwachtwoorden van leveranciers worden z.s.m. veranderd na installatie van systemen of programmatuur.
- Er is een overzicht bij het hoofd ICT beschikbaar van de medewerkers met administrator rechten en op welke systemen.
- Er vindt periodieke controle plaats (eenmaal per drie maanden) op de status van de medewerkers met administrator rechten.
- Een administrator recht wordt uitsluitend geautoriseerd door het hoofd ICT.

Technisch Beheer en proces

Instellingen voor technisch afdwingen wachtwoord- en toegangsbeveiligingsbeleid:

- Wachtwoordlengte en -complexiteit en geldigheid dient waar mogelijk technisch worden afgedwongen
- Een initieel afgegeven wachtwoord moet op eerste aanwijzing, in ieder geval binnen twee dagen na eerste keer gebruik van het systeem worden gewijzigd
- Wachtwoorden mogen niet in leesbare tekst worden getoond
- Het systeem is hoofdlettergevoelig (hoofdletter is een ander karakter dan een kleine letter)
- Er worden risico-beperkende technieken ingezet tegen onbeperkte inlog-pogingen, zoals o.a. vergrendelen van het account na aantal foutieve invoerpogingen.
Aanvullingen en/of aanpassing van de (instellingen van) deze technieken kunnen gedaan worden n.a.v. nieuwe inzichten, analyses en actuele bedreigingen en trends.

Controle en vaststelling

Gecontroleerd en geaccordeerd door:

- *Richard de Koning, Manager Informatieveiligheid en privacy*
- *Ronald Zeelenberg, Teamleider Centraal IT operatie*
- *Aladin Mhamdi, ICT Architect*

Vastgesteld op 28-10-2020 door:

- *Marcel van Oorschot, Functionaris Gegevensbescherming*