Wachtwoordbeleid
Gemeente Groningen

In opdracht van	Aaldert van Lingen (Directeur SSC-I&S)
Status	*Definitief*
Versie	1.0
Redacteur	Bas Verheijen (CISO)
Datum	08-11-2019

Versiebeheer			
Versie	***Datum***	***Wijzigingen***	***Auteur***
0.1	10-08-2018	Initiële versie, ter afstemming met Informatiebeveiligingsteam.	Bas Verheijen
0.2	04-10-2019	Distributie versie, ter vaststelling MT-I&S.	Bas Verheijen
1.0	08-11-2019	Definitieve versie.	Bas Verheijen

Goedkeuring				
Versie	***Datum***	***Naam***	***Functie***	***Status***
1.0	08-11-2019	Aaldert van Lingen	Directeur SSC-I&S	Definitief

Distributielijst		
Versie	***Datum***	***Naam***
0.1	10-08-2018	Interne review: - Informatiebeveiligingsteam. - Leverancier Fujitsu.
0.2	04-10-2019	Interne review: - MT-I&S.
1.0	08-11-2019	Gepubliceerd op intranet.

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Ten behoeve van de beveiliging van informatie binnen de systemen van de gemeente Groningen is dit aanvullend beleid er op gericht hoe met wachtwoorden omgegaan moet worden door zowel gebruikers als applicatie-/systeembeheerders.

In de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) worden eisen benoemd met betrekking tot wachtwoorden en beheersmaatregelen in relatie tot wachtwoorden. Dit document geeft de algemene aanwijzingen van de Informatiebeveiligingsdienst voor gemeenten (IBD) van de VNG over het omgaan met wachtwoorden. Deze aanwijzingen (versie 2.11, september 2019) zijn integraal overgenomen. Het versiebeheer van deze aanwijzingen voor de gemeente Groningen voor het wachtwoordbeleid berust bij de IBD. In het geval van aanvullende eisen die *specifiek* zijn voor de gemeente Groningen wordt dit *expliciet* vermeld. Ook verwijzingen naar de normen van de opvolger van de BIG, de Baseline Informatiebeveiliging Overheid (BIO) die vanaf 2019 wordt ingevoerd en verplicht is vanaf 2020, zijn aangegeven.

Dit document vormt het Wachtwoordbeleid van de gemeente Groningen en is een specifieke uitwerking van het Informatiebeveiligingsbeleid Gemeente Groningen dat is vastgesteld door alle betrokken partijen van de gemeente Groningen. Het is opgesteld door de Chief Information Security Officer (CISO), inhoudelijk beoordeeld binnen het Informatiebeveiligingsteam, intern afgestemd met de Informatiebeveiligingsraad en wordt gehanteerd om de specifieke regels met betrekking tot wachtwoorden uit te dragen.

1.2 Het belang van correcte omgang met wachtwoorden

Wachtwoorden vormen een belangrijk aspect van de informatiebeveiliging binnen de gemeente Groningen. Wachtwoorden zorgen ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot informatie die niet voor hen bestemd is. Een gemakkelijk wachtwoord evenals onduidelijke of niet gevolgde wachtwoordprocedures zijn een bedreiging voor de integriteit en vertrouwelijkheid van informatie en de privacy van burgers en bedrijven. Het kan zelfs leiden tot datalekken (met eventueel grote financiële consequenties) en is daarmee tevens slecht voor het imago van de gemeente Groningen.

Alle gebruikers van informatiesystemen in de gemeente Groningen dienen derhalve goede wachtwoorden te kiezen en zijn altijd zelf verantwoordelijk voor de geheimhouding van hun wachtwoorden en inloggegevens.

1.3 Raakvlakken

Er zijn meerdere onderdelen van de BIG die vanuit een verschillend perspectief (technisch en organisatorisch) eisen stellen aan de wachtwoorden zelf en het gebruik daarvan.

De volgende normen/maatregelen in de tactische variant van de BIG[1] hebben raakvlakken met dit onderwerp (de teksten/maatregelen die missen in de huidige voorzet van de IBD of alleen een *indirecte* relatie hebben met dit onderwerp zijn *cursief* weergegeven):

- *Maatregel 6.1.8 (Beoordeling van het informatiebeveiligingsbeleid)*

[1] De BI*O*-normen: 9.2.4, 9.3.1, 9.4.2 en 9.4.3 bevatten alle maatregelen die direct gerelateerd zijn aan wachtwoorden en bevatten geen aanvullende maatregelen ten opzichte van de BIG.

- Maatregel 9.2.1 (Leveranciers wachtwoorden)
- *Maatregel 10.10.1 (Aanmaken audit-logbestanden)*
- *Maatregel 10.10.2 (Controle van systeemgebruik)*
- Maatregel 11.2.3 (Beheer van wachtwoorden)
- Maatregel 11.3.1 (Gebruik van wachtwoorden)
- Maatregel 11.5.1 (Beveiligde inlogprocedures)
- Maatregel 11.5.2 (Gebruikers identificatie en authenticatie)
- Maatregel 11.5.3 (Systemen voor wachtwoordbeheer)
- Maatregel 11.7.1 (Draagbare computers *en communicatievoorzieningen*)
- Maatregel 12.1.1 (Beveiligingseisen ICT-systemen)
- *Maatregel 13.1.1 (Rapportage van informatiebeveiligingsgebeurtenissen)*
- *Maatregel 15.2.1 (Naleving van beveiligingsbeleid en -normen)*

1.4 Leeswijzer

In hoofdstuk 2 worden alle belangrijke facetten van wachtwoorden uiteengezet.

Hoofdstuk 3 geeft alle specifieke eisen weer voor het gebruik van wachtwoorden binnen de gemeente Groningen.

In bijlage A zijn ter volledigheid alle overige aan wachtwoorden gerelateerd BIG-normen benoemd en zijn waar nodig nader toegelicht.

In bijlage B is aangegeven welke (afwijkings-)informatie dient te worden geregistreerd om de technische eisen aan wachtwoorden aantoonbaar te kunnen beheersen en zo nodig als organisatie tijdelijk te gedogen.

2 Toelichting wachtwoorden

2.1 Algemeen

Een wachtwoord is een reeks tekens waarmee toegang wordt verkregen tot informatie, een computer of mobiel apparaat (zoals een smartphone, laptop of tablet). Naast wachtwoorden wordt er tegenwoordig ook steeds vaker de kans geboden om gebruik te maken van wachtwoordzinnen. Wachtwoordzinnen zijn meestal langer dan wachtwoorden met het oog op extra beveiliging en bevatten meerdere woorden die samen een zin vormen. Wachtwoordzinnen vragen vanwege hun lengte om veel meer ruimte in het invoervak of -veld. Wachtwoorden en wachtwoordzinnen helpen te voorkomen dat onbevoegde personen toegang krijgen tot bestanden, programma's en andere bronnen. Het is verstandig om sterke wachtwoorden te gebruiken voor alle gebruikers- en systeemaccounts. Een wachtwoord behoort altijd te zijn toegewezen aan een gebruikersaccount, die een fysieke gebruiker uniek identificeert. Alle handelingen van een gebruikersaccount moeten uniek kunnen worden toegewezen aan die gebruiker.

2.2 Eenmalige wachtwoorden versus statische wachtwoorden

Dit beleid gaat alleen over *statische* wachtwoorden, er bestaan echter ook nog *eenmalige* wachtwoorden (one time passwords). Een voorbeeld daarvan is het eenmalige wachtwoord dat gegenereerd kan worden door een token of door een applicatie. Denk aan Microsoft Authenticator of een wachtwoordtoken dat steeds een nieuwe reeks cijfers of cijfers en letters genereert. Dit laatste gebeurt dan op tijd of uit een bepaalde lijst.

2.3 Sterke en zwakke wachtwoorden

Wachtwoorden hebben een bepaalde sterkte nodig om het moeilijker te maken dat ze worden geraden of gekraakt. Dit kan door middel van bijvoorbeeld een brute force attack[2] of door middel van bestaande wachtwoordlijsten (rainbow tables). De sterkte van een wachtwoord wordt bepaald door de lengte, de complexiteit en de onvoorspelbaarheid. Zwakke wachtwoorden zijn vaak te kort of een te eenvoudig woord of te eenvoudige toetsencombinatie.

Het gebruiken van een sterk wachtwoord reduceert het risico dat het wachtwoord kan worden geraden. Er zijn echter ook maatregelen nodig om de beveiliging, die verkregen kan worden door het gebruik van wachtwoorden, in stand te houden.

Deze aanvullende maatregelen zijn:

- Het vaststellen van een beleid over wachtwoordgebruik binnen de organisatie, met daarin onder andere wachtwoordgeldigheid.
- Het implementeren van goede processen voor het verstrekken en het herstellen van wachtwoorden.
- De manier waarop in de applicaties wordt omgegaan met wachtwoorden.
- Medewerkers bewust maken dat wachtwoorden nooit gedeeld mogen worden.
- Wachtwoordsterktes technisch afdwingen.

Het vaststellen van een beleid

[2] Uit Wikipedia: Brute force (Engels voor "brute kracht") is het gebruik van rekenkracht om een probleem op te lossen met een computer zonder gebruik te maken van algoritmen of heuristieken om de berekening te versnellen. Brute force wordt gebruikt als er geen algoritme bekend is dat sneller of efficiënter tot een oplossing leidt. De methode bestaat uit het botweg uitproberen van alle mogelijke opties, net zolang tot er een gevonden is die overeenkomt met de gewenste invoer.

In hoofdstuk 3 is het specifieke wachtwoordbeleid van de gemeente Groningen uitgewerkt. Het is integraal, in lijn met het vastgestelde Informatiebeveiligingsbeleid Gemeente Groningen, gebaseerd op de BIG (en de BIO).

Verstrekken en wijzigingen van wachtwoorden

Het verstrekken en wijzigen van wachtwoorden dient met gestandaardiseerde processen te gebeuren. *Best practice* voorbeeld:

- Er komt een medewerker in dienst, de manager vraagt een gebruikersaccount aan bij ICT[3] (inclusief applicatietoegangsrechten), ICT maakt een nieuwe gebruikersaccount aan en verstrekt het wachtwoord op een veilige manier aan de nieuwe gebruiker. Dit tijdelijke wachtwoord moet de eerste keer dat het wordt gebruikt direct worden gewijzigd door de gebruiker. Denk hier ook aan een veilig wachtwoordwijzigingsproces voor het geval dat een medewerker zijn of haar wachtwoord vergeten is, zowel voor apparatuur en computersystemen als voor applicaties.

Applicaties en wachtwoorden

Functioneel applicatiebeheerders kunnen voor al hun applicaties zelf gebruikersnamen en wachtwoorden bijhouden in een (centrale) gebruikersaccountsdatabase. In deze database mogen wachtwoorden niet in klare (leesbare) taal staan. Standaard wordt van een wachtwoord een 'hash' gemaakt en opgeslagen. Tevens moet men deze hashwaarde extra beschermen door het toevoegen van een getal, de zogenaamde 'salt'[4]. Als een salt wordt gebruikt is het voor een aanvaller die de wachtwoordtabel weet te bemachtigen zo goed als niet meer mogelijk de wachtwoorden terug te berekenen of de tabellen te gebruiken. Er zijn speciale hashing algoritmes ontworpen zoals Argon2 en PBKDF2 die het bruteforcen van wachtwoorden op basis van de hash zo moeilijk en tijdrovend mogelijk maken.

Het aantal inlogpogingen is maximaal 5[5]. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.

2.4 Risico's in relatie tot wachtwoorden

Risico's die niet direct te maken lijken te hebben met wachtwoorden maar dat wel zijn:

- Afluisteren van het netwerk

Het versturen van wachtwoorden over onbeveiligde verbindingen (zoals http) is onveilig, omdat de wachtwoorden kunnen worden uitgelezen. Als netwerkverkeer kan worden afgeluisterd kan ook de *challenge response* (het vraag-antwoordprotocol) tussen systemen worden afgeluisterd. Daarmee kan informatie worden verkregen om wachtwoorden eenvoudig te raden en te gebruiken. Een tegenmaatregel kan zijn om gebruik te maken van *encrypted* (versleutelde) verbindingen.

[3] Binnen de context van gemeente Groningen is dit veelal het Shared Service Center (SSC), maar in het geval van systemen die buiten de netwerkomgeving van SSC, door andere leveranciers, gehost worden kan deze gebruikersbeheerdersrol elders, in de lijnorganisatie, belegd zijn.
[4] https://nl.wikipedia.org/wiki/Salt_%28cryptografie%29
[5] De BIG stelt 3 keer, maar 5 keer is geaccepteerd door gemeente Groningen. BIO-norm 9.4.3.1 gaat uit van 10 inlogpogingen, maar dat is gebruiksonvriendelijke indien gebruikgemaakt wordt van de wachtwoordherstelfunctionaliteit.

- Keyboard-loggers

Met een *keyboard-logger* wordt in dit geval een toetsenbordstekker bedoeld die tussen het toetsenbord en de PC wordt gestoken. Deze keyboard-loggers slaan alle toetsaanslagen op, en daarmee ook de ingetoetste gebruikersnamen en wachtwoorden. Er bestaan ook *softwarematige* keyboard-loggers. Een tegenmaatregel tegen *fysieke* keyboard-loggers is om regelmatig aan de buitenkant van de PC de toetsenbord aansluiting te controleren. De meeste antivirussoftware herkent de meeste softwarematige keyboard-loggers. Een maatregel tegen het risico van keyboard-loggers kan zijn om gebruik te maken van multifactorauthenticatie of eenmalige wachtwoorden.

- Phishing

Bij *phishing* wordt gebruik gemaakt van een e-mail waarbij de gebruiker wordt verleid om zijn de gegevens van zijn gebruikersaccount, de gebruikersnaam en het wachtwoord, in te vullen op een malafide website. Tegenmaatregelen die kunnen helpen zijn: gebruik maken van een goede up-to-date antivirusscanner en er dient aandacht te zijn voor het openen van e-mailbijlagen in informatiebeveiligingsbewustwordingscursussen. Multifactorauthenticatie helpt tegen phishing, mits de gebruiker niet verleid wordt om een eenmalig wachtwoord of tan-code af te geven.

- Social engineering

Een *social engineer* zal proberen gebruikersgegevens te krijgen door zich bijvoorbeeld voor te doen als helpdeskmedewerker. Er wordt dus gewoon om een gebruikersnaam en wachtwoord gevraagd en vaak gekoppeld aan een probleem dat moet worden opgelost. Een tegenmaatregel tegen social engineering is dat het geadresseerd moet zijn in informatiebeveiligingsbewustwordingscursussen. Een tegenmaatregel is ook dat er een waterdicht wachtwoordwijzigingsproces is, zodat een vreemde niet zomaar een wachtwoord kan laten wijzigen om zo toegang te krijgen tot systemen.

- Dumpster diving

Met *dumpster diving* wordt bedoeld dat iemand informatie verzameld door te zoeken in afval. Hier zit bijvoorbeeld informatie bij om een social engineering aanval uit te voeren. Een tegenmaatregel is dat voorkomen moet worden dat vuilnis makkelijk toegankelijk is en dat (gevoelige) informatie op papier wordt versnipperd/vernietigd.

- Shoulder surfing

Meekijken met het invoeren van wachtwoorden. Een tegenmaatregel is dat men zich bewust moet zijn van deze vorm van een aanval en dat men als gebruiker het meekijken over de schouder voorkomt. Een andere tegenmaatregel is een privacy-scherm bij de computer te gebruiken, dan wordt het in ieder geval moeilijker om mee te kijken op het scherm. Er bestaan ook oplossingen die het mogelijk maken om via biometrie in te loggen, hierdoor kunnen de inloggegevens niet over de schouder worden bekeken.

- Side-channel attacks

Met een *side-channel attack* wordt een aanval bedoeld, waarbij door het kijken naar bijvoorbeeld processortijd en stroomverbruik van hardware en software in cryptografiemodules zwakheden worden gevonden. Tegenwoordig wordt ook het afluisteren en analyseren van netwerkverkeer onder side-channel attacks begrepen, bijvoorbeeld het kraken van WEP of WPA van Wi-Fi-netwerken. Als netwerken gekraakt worden dan gebeurd dat door vaak genoeg het versleutelde wachtwoord op te vangen, waarna de overeenkomsten en de verschillen gebruikt worden om het wachtwoord te

herleiden. Hier kan men zich moeilijk tegen wapenen, een tegenmaatregel kan zijn dat het vermogen en de uitstraling van Wi-Fi naar buiten wordt beperkt.

- Softwarefouten

Door programmeerfouten in het schrijven van programma's kunnen er zwakheden worden geïntroduceerd, waardoor bijvoorbeeld wachtwoorden makkelijk te achterhalen zijn. Wachtwoorden die niet of met een zwak algoritme worden gesalt kunnen eenvoudiger gekraakt worden, waardoor de wachtwoorden zichtbaar worden. Een ander voorbeeld van een fout is dat webapplicaties gevoelig kunnen zijn voor *SQL-injectie*-aanvallen. Hierdoor kunnen bijvoorbeeld gebruikersnamen en wachtwoorden worden gelezen uit een tabel van de database, die bij de website hoort. Een tegenmaatregel kan zijn dat men software kwaliteitsprocessen invoert/handhaaft en software test voordat het in gebruik genomen wordt, bijvoorbeeld door een netwerkpenetratietest (pentest).

- Opschrijven van wachtwoorden

Wachtwoorden worden soms op briefjes opgeschreven en aan de monitor geplakt, of onder het toetsenbord of op een andere onveilige plaats bewaard. Dit dient geadresseerd te worden in informatiebeveiligingsbewustwordingscursussen. Een goed alternatief is het gebruikmaken van een wachtwoordmanager.

- Gecompromitteerde database

Regelmatig komt het voor dat er op internet gebruikersnamen en wachtwoorden worden gepubliceerd. Dit zijn gegevens uit gecompromitteerde databases. Het kan bijvoorbeeld zijn dat er een gemeentelijk e-mailadres in de database aanwezig is. Tegenmaatregelen kunnen zijn: regelmatig het wachtwoord wijzigen, andere wachtwoorden kiezen dan voor privédoeleinden, gebruik maken van tweefactorauthenticatie of van een eenmalige wachtwoordgenerator en gemeentelijke e-mailadressen alleen gebruiken voor zakelijke registraties op internet. Er zijn online websites te vinden die kunnen verifiëren of het gebruikersaccount / e-mailadres met een wachtwoord door een hack openbaar beschikbaar zijn[6].

2.5 Hoe kiest men sterke wachtwoorden

Sterke wachtwoorden zijn doorgaans niet zo gemakkelijk om te onthouden. Het is daarom beter om een wachtwoordzin te gebruiken die wel voor de gebruiker betekenis heeft. Als algemene regel geldt dat wachtwoordzinnen op grond van hun lengte veiliger zijn dan zogenaamd 'sterke' (complexe) wachtwoorden. Deze zin kan bijvoorbeeld de eerste regel uit een boek zijn.

Hoe gaat dit in zijn werk:

- Neem een zin die u kunt onthouden.
- Neem van ieder woord de eerste letter.
- Bijvoorbeeld: 'Onze gemeente is een veilige organisatie in 2019' wordt dan OGIEVOI2019. Als dan ook nog letters vervangen worden door leestekens en hoofd- en kleine letters worden gemixt ontstaat een erg moeilijk te kraken wachtwoord dat toch onthouden kan worden, het resultaat is dan: Og=€V0!2o19.
- Indien mogelijk / toegestaan kan ook de gehele zin ingevoerd worden.

[6] https://haveibeenpwned.com/

Zie de paragrafen 2.6 en 3.3 van dit beleid voor de wachtwoordregels op basis van de BIO. Indien er geen gebruikt wordt gemaakt van tweefactorauthenticatie dient de wachtwoordlengte minimaal 8 posities en complex van samenstelling te zijn. Als een wachtwoord minimaal 20 posities lang is dan vervalt de complexiteitseis.

2.6 Wachtwoordgedragsregels

Algemeen

- Gebruik verschillende wachtwoorden voor verschillende systemen/doelen, gebruik geen privé-wachtwoorden op het werk.
- Gebruik verschillende wachtwoorden voor verschillende applicaties op het werk, minimaal voor de essentiële[7] systemen die meer gevoelige informatie bevatten (indien geen gebruik gemaakt wordt van *single sign-on* (SSO)[8]).
- Gebruik altijd sterke wachtwoorden voor alle (maar zeker voor essentiële) systemen en wissel die regelmatig.
- Geef wachtwoorden aan niemand.
- Wachtwoorden mogen niet worden opgeschreven.
- Geef geen wachtwoorden door via e-mail, chat of andere elektronische communicatiekanaal en als dat toch moet, dan gescheiden (via een andere weg) van de gebruikersnaam.
- Geef geen al te gemakkelijke hints of controlevraag over het wachtwoord, bijvoorbeeld je naam of de meisjesnaam van je moeder.
- Geef nooit een wachtwoord op voor onderzoeken, vragen van anderen of om iemand te helpen, het vragen om een wachtwoord moet worden aangemerkt als een informatiebeveiligingsincident. Dit dient te worden gemeld aan de binnen de organisatie door die organisatie zelf vastgestelde persoon (binnen de gemeente via de ICT-servicedesk aan de CISO).
- Maak geen gebruik van de 'wachtwoord-onthoud'-functie van sommige webbrowsers.
- Maak geen gebruik van de functie om ingelogd te blijven.
- Wijzig een wachtwoord direct bij vermoeden van misbruik en meld het aan de ICT-servicedesk, zodat zij de juiste maatregelen kunnen nemen.
- Wachtwoorden van gebruikersaccounts moeten niet worden gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro).
- Bij een grote hoeveelheid inlogaccounts en wachtwoorden is het aan te bevelen om deze op te slaan in een daarvoor bedoelde veilige applicatie of app (paragraaf 2.7).

Aanwijzingen voor applicaties en applicatieontwikkeling

- Wachtwoorden worden uitsluitend gebruikt voor natuurlijke en unieke aanwijsbare personen en systemen, indien mogelijk moet het gebruik van groepsaccounts worden vermeden.
- Wachtwoorden mogen niet in klare (leesbare) taal of ongezouten (*un salted*) worden opgeslagen.
- Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.

[7] Systemen met een hoge score op de kwaliteitsaspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid: kortweg de BIV-classificatie.
[8] https://nl.wikipedia.org/wiki/single_sign-on.

2.7 Wachtwoordmanagers

Wachtwoordmanagers[9] worden steeds vaker gebruikt. Een wachtwoordmanager is een applicatie om wachtwoorden te beheren. In de applicatie kunnen de huidige wachtwoorden worden opgeslagen, maar ook nieuwe 'sterke' wachtwoorden aangemaakt worden. Om de applicatie te gebruiken hoeft de gebruiker maar één wachtwoord te onthouden. Dit wachtwoord geeft toegang tot de in een database opgeslagen wachtwoorden. Er zijn twee categorieën wachtwoordmanagers: centraal beheerd en stand-alone (online en offline varianten). Zakelijk gezien kan het gebruik van een centraal beheerde wachtwoordmanager nog meer voordelen opleveren, omdat ook bij vertrek of rol-/functiewijziging gelijk de toegang tot applicaties/informatie kan worden ontnomen of aangepast. Ook kunnen wachtwoordregels per applicatie/toegang beter afgedwongen worden en doorgaans auditproof gelogd worden. Wachtwoordmanagers worden bij voorkeur gebruikt met tweefactorauthenticatie en een unlock-time na succesvolle authenticatie, dat wil zeggen dat de wachtwoordmanager na een bepaalde tijd weer op slot gaat. Een wachtwoordkluis dient beschikbaar gesteld te worden aan de medewerkers.

2.8 Multifactorauthenticatie

Een normaal gebruikersaccount kent een gebruikersnaam en een wachtwoord, dit noemen we vaak: 'iets wat je *weet*'. Tweefactorauthenticatie voegt daar een extra dimensie aan toe: 'iets wat je *hebt*' of 'iets wat je *bent*'. In het eerste geval heeft men het dan over verschillende soorten tokens: USB-token, een key-/nummergenerator, een sms-code. In het tweede geval heeft men het dan over de biometrische[10] kenmerken van een persoon, de meest gangbare zijn: een vingerafdruk, een gelaat- of irisscan of je stem. Naast het wachtwoord wordt er om een extra verificatiemethode gevraagd[11]. Door tweefactorauthenticatie te gebruiken wordt het voor kwaadwillenden moeilijker om toegang te krijgen tot een account. Tweefactorauthenticatie geeft een extra zekerheid dat de persoon die inlogt ook daadwerkelijk diegene is die toegang mag hebben. Voor heel erg streng beveiligde systemen spreekt men soms ook nog van driefactorauthenticatie, in dit geval wordt gebruik gemaakt van iets wat je *weet* (gebruikersnaam en wachtwoord), iets wat je *hebt* (token) en iets wat je *bent* (biometrie). Door de komst van meer (mobiele) locatie-informatie kan ook gebruik worden gemaakt van een vierde factor: *waar* je met je inlogapparatuur bent. Deze laatste factor kan bijvoorbeeld worden gebruikt om uit te sluiten dat vanuit huis de BRP (en niet alleen vanaf de publieksbalie) kan worden benaderd, terwijl je wel rechten hebt om te telewerken met alle andere applicaties. In situaties waar geen tweefactorauthenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd[12].

2.9 Controle van wachtwoorden

Minimaal eens per 60 dagen worden wachtwoorden gewijzigd. Waar mogelijk worden wachtwoordeisen technisch afgedwongen[13], dit dient minimaal eens per jaar te worden gecontroleerd.

---

[9] https://www.nctv.nl/binaries/Factsheet%20gebruik%20tweefactorauthenticatie_tcm31-242994.pdf
[10] Alleen gebruik maken van éénfactorauthenticatie op basis van biometrische kenmerken is sterk af te raden, aangezien deze (normaalgesproken) niet gewijzigd kunnen worden.
[11] BIO-norm 9.4.2.1. eist tweefactorauthenticatie bij benadering van het netwerk / applicaties vanuit een onvertrouwde zone (alles buiten de fysieke (ICT-)infrastructuur van de gemeente Groningen).
[12] Idem.
[13] BIO-norm 9.4.3.3.

Wachtwoordbeleid dient zo veel als mogelijk binnen (informatie-)systemen te worden afgedwongen. De resultaten van de controle en de gevonden afwijkingen door de applicatie-/systeemeigenaar dienen te worden gerapporteerd via de planning- & controlcyclus aan het management en de CISO zodat maatregelen kunnen worden genomen om fouten te herstellen.
Voor (informatie)-systemen die voldoen aan het wachtwoordbeleid geldt een maximale geldigheidsduur van een jaar en daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.

2.10 Afwijkingen ten opzichte van de BIG-normen

Het uitgangspunt is dat alle applicaties die intern en extern door de gemeente Groningen worden gebruikt voldoen aan de minimumeisen vanuit de BIG[14].
Jaarlijks dient dit te worden vastgesteld. Omdat er mogelijkerwijs oude, nog in gebruik zijnde applicaties (legacy) bestaan die technisch niet (kunnen) voldoen, dient dit door de applicatie-/systeemeigenaar met een expliciete onderbouwing in de vorm van een risicoanalyse aan de CISO te worden verantwoord. Periodiek (jaarlijks) dient te worden vastgesteld of en tot wanneer de desbetreffende applicatie nog nodig is (zodat deze formeel kan worden gedoogd en vervolgens uitgefaseerd), dan wel kan worden aangepast zodat deze aan de minimumwachtwoordeisen kan gaan voldoen.

In bijlage B staat een overzicht dat jaarlijks door de applicatie-/systeemeigenaren dient te worden bijgewerkt om vast te stellen welke applicaties uit het technisch afwijkings-/gedoogregister kunnen. Dit overzicht dient voor alle *intern*[15] beheerde applicaties te worden bijgehouden voor het Shared Service Center (SSC) in de *configuration management database* (CMDB[16]) door de systeemeigenaar.

[14] Vanaf 1 januari 2020 de BIO.
[15] Dit geldt ook voor de SaaS-applicaties die kunnen worden geconfigureerd door de gemeente Groningen.
[16] ServiceNow.

3 Wachtwoordbeleid Gemeente Groningen

3.1 Beleidsuitgangspunten voor het gebruik van wachtwoorden in de gemeente Groningen

Ten behoeve van de beveiliging van informatie binnen gemeentelijke systemen is dit beleid er op gericht hoe met wachtwoorden omgegaan moet worden. Wachtwoorden vormen een belangrijk aspect van de gemeentelijke informatiebeveiliging. Wachtwoorden zorgen ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot gemeentelijke informatie. Een gemakkelijk wachtwoord evenals onduidelijke of niet gevolgde wachtwoord procedures zijn een bedreiging voor de vertrouwelijkheid en integriteit van gemeentelijke informatie, maar uiteindelijk ook voor het imago van de gemeente. Alle gebruikers van gemeentelijke informatiesystemen dienen goede wachtwoorden te kiezen en zijn verantwoordelijk voor de geheimhouding van hun wachtwoorden en inloggegevens.

De gemeente Groningen hanteert de volgende beleidsuitgangspunten die integraal zijn ontleend aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)[17] en de operationele producten van de Informatiebeveiligingsdienst (IBD) van de VNG.

Het doel van dit wachtwoordbeleid is drieledig:
- Het vaststellen van regels waar wachtwoorden en wachtwoordprocedures aan moeten voldoen.
- Het vaststellen van de bescherming van de wachtwoorden.
- Het vaststellen van de wijzigingscriteria voor wachtwoorden.

Omdat regelmatig vragen over wachtwoorden worden gesteld zijn hieronder de desbetreffende *letterlijke* normen vanuit de BIG en referenties naar de BIG-normen vermeld. Daar waar nodig is enige toelichting tussen vierkante haken **[...]** toegevoegd.

3.2 Algemeen wachtwoordbeleid

1. Standaard leverancierswachtwoorden, die in systemen zitten, worden voor ingebruikname gewijzigd. [Norm 9.2.1 - Plaatsing en bescherming van apparatuur].

2. Wachtwoorden worden nooit in originele vorm (plaintext / klare leesbare tekst) opgeslagen of verstuurd, maar in plaats daarvan wordt bijvoorbeeld de hashwaarde van het wachtwoord gecombineerd met een salt opgeslagen. [Norm 11.2.3 - Beheer van gebruikerswachtwoorden].
   Ten aanzien van wachtwoorden geldt:
   - Wachtwoorden worden op een veilige manier uitgegeven (authenticatie: controle van de identiteit van de gebruiker).
     i. [Dit is binnen de gemeente Groningen vooral relevant bij de telefonische uitgifte of het herstellen van wachtwoorden door de ICT-servicedesk of door functioneel applicatiebeheerders. In principe geldt voor het netwerkaccount dat de wachtwoordherstelfunctionaliteit via de applicatie IDaaS[18] als primair wachtwoordherstelproces dient te worden gebruikt door alle medewerkers. Deze applicatie is 24x7 beschikbaar via internet en vanaf elk apparaat bruikbaar, zonder tussenkomst van collega's].

[17] Vanaf 1 januari 2020 de BIO.
[18] De applicatie *Identity as a Service* (IDaaS) zal begin 2020 worden aangeboden aan de gemeente Groningen.

- Tijdelijke wachtwoorden of wachtwoorden die standaard in software of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord. Tijdelijke wachtwoorden zijn maximaal een werkdag geldig.
  i. [Bij zowel een nieuwe gebruikersaccount als bij een wachtwoordherstel het wachtwoord, waar mogelijk technisch afgedwongen, laten wijzigen].
- Gebruikers bevestigen de ontvangst van een wachtwoord.
  i. [In het geval van fysieke overdracht van een wachtwoord].
- Wachtwoorden zijn alleen bij de gebruiker bekend.
- Zonder tweefactorauthenticatie dienen wachtwoorden te bestaan uit minimaal **8 vrij te kiezen karakters**[19], waarvan tenminste 1 kleine letter, 1 hoofdletter, 1 cijfer en 1 vreemd teken. Bij meer dan 20 karakters vervalt de complexiteitseis.
- Wachtwoorden zijn maximaal een jaar geldig indien de (informatie)-systemen voldoen aan het wachtwoordbeleid. Anders zijn de wachtwoorden maximaal 6 maanden geldig.
- Wachtwoorden zijn maximaal **90 dagen**[20] geldig en mogen niet binnen 6 keer herhaald worden.
  i. [Wachtwoordhistorie is derhalve minimaal 6 wachtwoorden].
- Het aantal foutieve inlogpogingen staat op **maximaal 5 keer**[21], daarna wordt het account inactief.

3.3 Wachtwoorden voor alle gebruikers

Gebruikers behoren goede beveiligingsgewoonten in acht te nemen bij het kiezen en gebruiken van wachtwoorden. [Norm 11.3.1 - Gebruik van wachtwoorden].

1. Aan de gebruikers is een set *gedragsregels* aangereikt met daarin minimaal het volgende:
   - Wachtwoorden worden niet opgeschreven.
   - Gebruikers delen hun wachtwoord nooit met anderen.
   - Wachtwoorden mogen niet opeenvolgend zijn.
   - Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde.
   - Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro).
   - Misbruik van wachtwoorden dient als beveiligingsincident gemeld te worden aan de ICT-servicedesk.
   - Nadat voor een gebruikersnaam **vijf[22] keer** een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker een verzoek indient deze lock-out op te heffen of het wachtwoord te herstellen volgens de geldende wachtwoordherstelprocedure. [Norm 11.5.1 - Beveiligde inlogprocedures].

[19] BIO-norm 9.4.3.1.
[20] De BIG stelt maximaal 60 dagen, maar vanwege gebruikersgemak heeft gemeente Groningen het risicogeaccepteerd voor de Active Directory (door middel van RAO-2018-092).
BIO-norm 9.4.3.1. stelt minimaal halfjaarlijks wijzigen indien *geen* tweefactorauthenticatie plaatsvindt.
[21] De BIG stelt maximaal 3 keer. BIO-norm 9.4.3.1. gaat uit van 10 inlogpogingen. Dat is echter gebruiksonvriendelijk indien gebruikgemaakt wordt van de wachtwoordherstelfunctionaliteit, derhalve is gekozen voor 5 keer.
[22] Idem.

2. Binnen de gemeente Groningen wordt de optie van een eigen wachtwoordmanager (of wachtwoordkluis[23]) aangeboden aan medewerkers die met veel verschillende (beheer)wachtwoorden werken. Hiervoor wordt gebruik gemaakt van de applicatie *KeePass*.

3.4 Aanvullend beleid voor wachtwoorden van systeembeheerders

Toegang tot besturingssystemen van de gemeente Groningen behoort te worden beheerst met een beveiligde inlogprocedure. [Norm 11.5.1 - Beveiligde inlogprocedures].

1. Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van tweefactorauthenticatie.[24]

2. Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.

3. Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.

4. Bij een succesvol inlogproces wordt de datum en tijd van de voorgaande inlog of inlogpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.

5. Voor mobiele apparaten wordt de *wipe*-functie (het op afstand wissen van de gegevens op het apparaat) automatisch geactiveerd bij vaker dan **10 maal**[25] foutief inloggen.

3.5 Wachtwoordbeheer

Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen. [Norm 11.5.3 - Systemen voor wachtwoordenbeheer].

1. Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden[26], regelmatige wijziging, directe wijziging van initieel wachtwoord).

2. Wachtwoorden hebben een geldigheidsduur zoals beschreven in maatregel 11.2.3[27] van de BIG. Binnen deze tijd dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.

[23] BIO-norm 9.3.1.1.
[24] Met tweefactorauthenticatie wordt hier bedoelt: iets dat je *weet* (je wachtwoord) en iets dat je *hebt* (bijvoorbeeld een mobiele telefoon, token of key-/nummergenerator).
[25] Vastgesteld als maximum op basis van een risico-inschatting van gemeente Groningen in 2019. Dit is een afwijking ten opzichte van het voorbeeld wachtwoordbeleid van de VNG-IBD (dat uitgaat van 5 maal, maar zij laat het exacte aantal vrij aan gemeenten).
[26] Een voldoende sterk wachtwoord is een wachtwoord waarvan de entropie hoog is. Deze is afhankelijk van de lengte en het aantal mogelijke tekens. Zie ook 'The true costs of unusable password policies', en Gartner research note G00124970 (http://www.indevis.de/dokumente/gartner_passwords_breakpoint.pdf
[27] BIO-norm 9.4.3.5.

3. Wachtwoorden die hersteld zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur[28] en moeten bij het eerste gebruik worden gewijzigd.

4. De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende:
    - Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd.
    - *Ter voorkoming van typefouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure.*

3.6 Controle en rapportage

Applicatie-/systeemeigenaren controleren bij alle nieuwe informatiesystemen en minimaal eens per jaar bij alle bestaande informatiesystemen of de wachtwoordinstellingen nog juist (in lijn met het wachtwoordbeleid) zijn.

De uitkomsten worden binnen de gemeente Groningen via de P&C-cyclus gerapporteerd aan de CISO en het management.

[28] BIO-norm 9.4.3.4. stelt een expliciet maximum geldigheidsduur van één werkdag.

Bijlage A – Overige zijdelings gerelateerde BIG-normen

Norm 6.1.8 – Beoordeling van het informatiebeveiligingsbeleid

De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (dat wil zeggen beheerdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich wijzigingen voordoen in de implementatie van de beveiliging.

3. Over het functioneren van de informatiebeveiliging wordt, conform de P&C-cyclus, jaarlijks gerapporteerd aan het lijnmanagement.

[Periodiek (minimaal jaarlijks) worden alle beveiligingsinstellingen, waaronder de wachtwoordinstellingen, aangetoond].

Norm 10.10.1 – Aanmaken audit-logbestanden

Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.

3. [A] In een log-regel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, enzovoort).

Norm 10.10.2 – Controle van systeemgebruik

Er behoren procedures te worden vastgesteld om het gebruik van ICT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.

1. De volgende gebeurtenissen worden in ieder geval opgenomen in de logging:
   - Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord herstellen, uitgifte en intrekken van cryptosleutels.
   - Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities of kwetsbaarheden, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services).
   - Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.

Norm 11.5.2 – Gebruikersidentificatie en -authenticatie

Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.

2. Bij het intern gebruik van ICT-voorzieningen worden gebruikers minimaal geauthenticeerd op basis van wachtwoorden.

Norm 11.7.1 – Draagbare computers en communicatievoorzieningen

Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.

1. [A] Het mobiele apparaat is waar mogelijk zo ingericht dat geen bedrijfsinformatie wordt opgeslagen (‘zero footprint’). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, geldt: een mobiel apparaat (zoals een handheld computer, tablet, smartphone, PDA) biedt de mogelijkheid om de toegang te beschermen door middel van een wachtwoord en versleuteling van die gegevens. Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats.

Norm 12.1.1 – Analyse en specificatie van beveiligingseisen

In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.

6. Er is expliciet aandacht voor leveranciersaccounts, hardcoded wachtwoorden en mogelijke ‘achterdeurtjes’.

Norm 13.1.1 – Rapportage van informatiebeveiligingsgebeurtenissen

Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.

6. Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De CISO bekijkt periodiek - bij voorkeur maandelijks - een samenvatting van de informatie.

Norm 15.2.1 – Naleving van beveiligingsbeleid en -normen

Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.

2. [A] In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging aan de hand van het in control statement.

[Idem norm 6.1.8: Periodiek (minimaal jaarlijks) worden alle beveiligingsinstellingen, waaronder de wachtwoordinstellingen, aangetoond].

Bijlage B – Voorbeeld technisch afwijkings-/gedoogregister wachtwoorden (CMDB)

Organisatie/Afdeling	**Applicatienaam (+ leverancier)**	**Naam primair proces**	**Technische afwijking wachtwoordinstelling**	**Compenserende maatregel(en)**	**Laatste toetsdatum**
Gemeente Groningen	…	…	*Op BIG-norm X.X.X: …*	…	*2019-XX-XX*
Sociaal Domein	GWS4all (Centric)	Alle processen waarin GWS4all gebruikt wordt.	Op BIG-norm 11.2.3 (Wachtwoordsterkte: maximale geldigheidsduur van wachtwoorden wordt niet afgedwongen).	Handmatige controle door functioneel beheer van GWS4all.	2019-XX-XX
Sociaal Domein	MKS (Makelaarssuite)	Proces X en Y.	Gebruikers kunnen LDAP-wachtwoord niet wijzigen in de huidige versie.	RAO-2019-103.	2018-12-31
Stichting WIJ					
Noordelijk Belasting Kantoor					
Gemeenschappelijke Regeling XXX					