|  |
| --- |
| Richtlijn WachtwoordenTemplate |

|  |  |
| --- | --- |
| Auteur(s): |  |
| Versie: |  |
| Datum: | Kies of typ een datum |
| Kenmerk: |  |
|  |  |
|  |  |

**Documentinformatie**

Dit document maakt onderdeel uit van een complete set (beleidspiramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag Richtlijn in de beleidspiramide.



**Versiebeheer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Verwerking** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Distributielijst**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Ontvanger** | **Doel** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Vastgesteld door** | **Vastgesteld op** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Samenhang met andere documenten**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Bovenliggend** | **Gelijk niveau** | **Onderliggend** |
| [INFORMATIEBEVEILIGINGSBELEID] | x |  |  |
| [STANDAARD IDENTITEIT EN TOEGANGSBEHEER] | x |  |  |
| [DIVERSE RICHTLIJNEN] |  | x |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | ID.01, ID.02, ID.04, SM.03, SM.13 |
| ISO27001:2022 | A5, A6, A7, A8 |

**Creative Commons**

Dit template is een product van het SURF Security Expertise Centrum en beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal. <https://creativecommons.org/licenses/by/4.0/deed.nl>

Inhoudsopgave

|  |
| --- |
| [Samenvatting 4](#_Toc195791609)[1 Inleiding 5](#_Toc195791610)[1.1 Doel 5](#_Toc195791611)[1.2 Reikwijdte en Toepassingsgebied 5](#_Toc195791612)[1.3 Rollen en Verantwoordelijkheden 5](#_Toc195791613)[1.4 Definities en Terminologie 6](#_Toc195791614)[2 Algemene principes voor Wachtwoorden 7](#_Toc195791615)[2.1 Het belang van sterke wachtwoorden 7](#_Toc195791616)[2.2 Risico’s van zwakke wachtwoorden 7](#_Toc195791617)[2.3 Beveiligingsoverwegingen bij wachtwoordgebruik 7](#_Toc195791618)[2.4 Multi Factor Authenticatie (MFA) 7](#_Toc195791619)[3 Richtlijn Wachtwoorden 8](#_Toc195791620)[3.1 Algemene vereisten voor wachtwoorden 8](#_Toc195791621)[3.2 Vereisten voor gewone gebruikersaccounts 8](#_Toc195791622)[3.3 Vereisten voor accounts met extra rechten 9](#_Toc195791623)[3.4 Vereisten voor serviceaccounts 9](#_Toc195791624)[3.5 Vereisten voor wachtwoordbeheer en -opslag 9](#_Toc195791625)[4 Audit en monitoring van Wachtwoordgebruik 10](#_Toc195791626)[4.1 Periodieke audits van wachtwoordbeveiliging 10](#_Toc195791627)[4.2 Registratie en bewaking van beheerdersactiviteiten 10](#_Toc195791628)[4.3 Detectie van ongebruikelijke toegangspatronen 10](#_Toc195791629)[4.4 Rapportage van beveiligingsincidenten 11](#_Toc195791630)[5 Opleiding en Bewustwording 12](#_Toc195791631)[5.1 Training en continue bewustwording 12](#_Toc195791632)[5.2 Wijzigen van zwakke wachtwoorden 12](#_Toc195791633)[6 Vaststelling 13](#_Toc195791634) |

Samenvatting

Hier komt een samenvatting, op zichzelf leesbaar, van de inhoud van dit document in max. 1 A4.

# Inleiding

Wachtwoorden zijn een belangrijk onderdeel van de beveiliging van systemen en gegevens binnen onze instelling. Een zorgvuldig wachtwoordbeleid helpt de risico’s op ongeautoriseerde toegang te beperken en draagt bij aan een veilige werkomgeving. Dit document beschrijft de vereisten voor het gebruik en beheer van wachtwoorden en sluit aan op onze ‘Standaard Identiteit en Toegangsbeheer’.

Deze richtlijn is gebaseerd op internationaal erkende normen, waaronder ISO 27001:2022, het SURFaudit Toetsingskader en de CIS Controls. Hierin worden de eisen en richtlijnen vastgelegd voor wachtwoordgebruik binnen onze instelling, inclusief het gebruik van wachtwoordkluizen en aanvullende maatregelen voor accounts met verhoogde rechten.

## Doel

Deze richtlijn heeft tot doel uniforme en afdwingbare eisen vast te stellen voor het gebruik en beheer van wachtwoorden binnen onze instelling. Het beschrijft onze principes voor o.a.:

* Het waarborgen van minimale vereisten voor wachtwoordsterkte en complexiteit;
* Het implementeren van beveiligingsmaatregelen voor accounts met aanvullende rechten;
* Het vaststellen van richtlijnen voor het gebruik en beheer van wachtwoordkluizen;
* Het verduidelijken van verplichtingen en verantwoordelijkheden van gebruikers en beheerders.

Door deze richtlijn toe te passen, wordt de kans op ongeautoriseerde toegang verkleind en wordt voldaan aan de geldende beveiligingsstandaarden.

## Reikwijdte en Toepassingsgebied

Deze richtlijn is van toepassing op alle IT-systemen, applicaties en diensten binnen onze instelling waarbij wachtwoorden worden gebruikt voor authenticatie. Dit omvat:

* Medewerkers, studenten, externe en andere gebruikers met toegang tot IT-systemen;
* Gewone gebruikersaccounts en accounts met aanvullende rechten, zoals beheer- en systeemaccounts;
* Het gebruik en beheer van een wachtwoordkluis;
* Alle wachtwoorden die worden gebruikt voor toegang tot systemen en gegevens, ongeacht de locatie of het apparaat waarmee toegang wordt verkregen.

Andere vormen van authenticatie, zoals certificaten of biometrische methoden, vallen buiten de scope tenzij deze in combinatie met wachtwoorden worden gebruikt.

## Rollen en Verantwoordelijkheden

Iedere gebruiker binnen onze instelling is verantwoordelijk voor het naleven van de vastgestelde wachtwoordregels. Dit houdt in:

* Het kiezen en gebruiken van wachtwoorden volgens de gestelde eisen;
* Het beveiligen van wachtwoorden tegen ongeoorloofd gebruik of delen met anderen;
* Het correct gebruik van een wachtwoordkluis indien vereist;
* Het direct melden van (vermoedelijk) compromitteren van wachtwoorden bij de verantwoordelijke afdeling.

Beheerders en systeembeheerders hebben aanvullende verantwoordelijkheden:

* De implementatie en handhaving van het wachtwoordbeleid binnen IT-systemen;
* Het instellen van technische maatregelen zoals wachtwoordbeleid en accountvergrendeling;
* Het monitoren en loggen van beveiligingsincidenten die verband houden met wachtwoordgebruik.

## Definities en Terminologie

Binnen deze richtlijn worden de volgende definities gehanteerd:

* **Gewoon gebruikersaccount**
Een account dat toegang biedt tot standaardfunctionaliteiten zonder aanvullende beheerrechten.
* **Account met aanvullende rechten**
Een account met verhoogde bevoegdheden, zoals een beheerders- of supergebruikersaccount.
* **Multi-Factor Authenticatie (MFA)**
Een authenticatiemethode waarbij meerdere factoren worden gebruikt om de identiteit van een gebruiker te verifiëren.
* **Wachtwoordkluis**
Een applicatie of dienst waarmee wachtwoorden veilig worden opgeslagen en beheerd.
* **Standaard Identiteit en Toegangsbeheer**
De overkoepelende standaard waarin de richtlijnen voor identiteits- en toegangsbeheer binnen onze instelling zijn vastgelegd.

# Algemene principes voor Wachtwoorden

Het gebruik van sterke wachtwoorden is noodzakelijk om de risico’s van ongeautoriseerde toegang te minimaliseren. Dit hoofdstuk beschrijft de algemene principes voor het instellen, beheren en beveiligen van wachtwoorden binnen onze instelling. Wachtwoorden moeten voldoende complex zijn, regelmatig worden geëvalueerd en aangevuld worden met aanvullende beveiligingsmaatregelen zoals multi-factor authenticatie (MFA)[[1]](#footnote-2).

## Het belang van sterke wachtwoorden

Een goed wachtwoord is moeilijk te raden of te kraken en voldoet aan de vastgestelde eisen voor lengte, complexiteit en uniek gebruik per systeem of dienst. Gebruikers moeten vermijden wachtwoorden te hergebruiken of voorspelbare patronen te hanteren.

Hoofdstuk 3 Richtlijn wachtwoorden beschrijft de minimale vereisten voor het gebruik van wachtwoorden binnen onze instelling.

## Risico’s van zwakke wachtwoorden

Een wachtwoord is de eerste laag in toegangsbeveiliging. Zwakke wachtwoorden vormen daarom een aanzienlijk risico voor de beveiliging. Veelvoorkomende problemen zijn te korte wachtwoorden, het gebruik van veelvoorkomende woorden of combinaties en hergebruik van wachtwoorden over meerdere systemen. Aanvallers maken gebruik van technieken zoals brute-force-aanvallen en woordenlijsten om zwakke wachtwoorden te achterhalen. Door zwakke wachtwoorden te vermijden, wordt het risico op ongeautoriseerde toegang beperkt.

## Beveiligingsoverwegingen bij wachtwoordgebruik

Naast het kiezen van een sterk wachtwoord moeten gebruikers en beheerders aanvullende maatregelen nemen om wachtwoorden te beschermen. Dit omvat o.a.:

* Het niet opschrijven van wachtwoorden op onbeveiligde locaties.
* Het gebruik van een wachtwoordkluis[[2]](#footnote-3) voor het veilig opslaan en beheren van wachtwoorden wordt aangeraden voor gewone gebruikersaccounts en is verplicht voor accounts met extra rechten en/of kritische rollen.
* Het periodiek controleren en bijwerken van wachtwoorden indien nodig.
* Het beperken van inlogpogingen om brute-force-aanvallen tegen te gaan.
* Het vermijden van wachtwoorddeling of -hergebruik binnen en buiten de instelling.

## Multi Factor Authenticatie (MFA)

MFA voegt een extra laag beveiliging toe aan het authenticatieproces. Naast een wachtwoord moet de gebruiker een aanvullende verificatiemethode gebruiken, zoals een tijdsgebonden code, biometrische gegevens of een hardware token. Dit verkleint de kans dat een aanvaller met alleen een wachtwoord toegang krijgt.

Binnen onze instelling is MFA verplicht voor alle accounts, zoals beschreven in de ‘Richtlijn MFA’. Gebruikers en beheerders dienen de richtlijnen uit dat document te volgen bij de implementatie en het gebruik van MFA.

# Richtlijn Wachtwoorden

Dit hoofdstuk beschrijft de minimale vereisten voor het gebruik van wachtwoorden, onderverdeeld in gewone gebruikersaccounts, accounts met extra rechten en het beheer en de opslag van wachtwoorden.

## Algemene vereisten voor wachtwoorden

Deze sectie beschrijft de algemene eisen die gelden voor alle typen accounts binnen onze instelling.

**Vereisten**

* Wachtwoorden moeten minimaal 15 tekens lang zijn.
* Wachtwoorden moeten voldoen aan complexiteitsregels: combinatie van hoofdletters, kleine letters, cijfers en speciale tekens.
* Alle gebruikers moeten hun wachtwoorden controleren tegen een lijst van bekende gelekte wachtwoorden; alleen wachtwoorden die niet in deze lijst voorkomen, mogen worden gebruikt.[[3]](#footnote-4)
* De tekenset voor wachtwoorden is UTF-8.
* Wachtwoorden mogen niet zichtbaar zijn tijdens invoer, tenzij de gebruiker dit expliciet activeert.
* Wachtwoorden worden gehasht en gesalt volgens NIST-normen en mogen nooit in reversibele vorm worden opgeslagen.
* Wachtwoorden mogen niet opnieuw worden gebruikt binnen een periode van ten minste vijf vorige wachtwoorden.
* Accounts moeten na een bepaald aantal mislukte inlogpogingen tijdelijk worden geblokkeerd of alternatieve rate-limiting maatregelen toepassen (zoals CAPTCHA).
* Wijzigingen aan authenticatiefactoren mogen alleen plaatsvinden na voldoende verificatie van de identiteit van de gebruiker.
* Multi-Factor Authenticatie (MFA) is verplicht voor alle gebruikersaccounts, volgens de 'Richtlijn MFA'.

## Vereisten voor gewone gebruikersaccounts

Naast de algemene vereisten gelden de volgende specifieke eisen voor gewone gebruikersaccounts:

**Vereisten**

* Gebruikers kiezen hun eigen wachtwoorden; initiële of reset-wachtwoorden moeten direct na de eerste login gewijzigd worden.
* Een indicator van wachtwoordsterkte wordt getoond bij het instellen van een nieuw wachtwoord.
* Persoonlijke accounts moeten een traceerbare eigenaar hebben die verantwoordelijk is voor het beheer van het wachtwoord.
* Wachtwoorden mogen niet gedeeld worden met andere gebruikers.

## Vereisten voor accounts met extra rechten

Accounts met verhoogde rechten (beheerdersaccounts) vereisen extra beveiligingsmaatregelen.

**Vereisten**

* Wachtwoorden moeten worden opgeslagen in een wachtwoordkluis met versleuteling en MFA.
* Wachtwoorden van beheerdersaccounts moeten regelmatig worden gewijzigd en mogen niet gelijk zijn aan persoonlijke gebruikerswachtwoorden.
* Administratieve taken moeten bij voorkeur worden uitgevoerd met tijdelijke verhoogde rechten in plaats van een permanent verhoogd account.
* Toegang tot beheerdersaccounts wordt periodiek geëvalueerd en continu gemonitord.

## Vereisten voor serviceaccounts

Serviceaccounts worden o.a. gebruikt voor geautomatiseerde processen en vereisen specifieke maatregelen. Onder deze categorie vallen ook de systeem accounts.

**Vereisten**

* Serviceaccounts mogen alleen worden gebruikt voor systeem- of applicatie-authenticatie en niet voor menselijke interactie.
* Serviceaccounts moeten een unieke documentatie en eigenaar hebben.
* Elk serviceaccount heeft een unieke aanmeldingsnaam en wordt geregistreerd in de CMDB.
* Service account-wachtwoorden moeten minimaal 32 tekens lang zijn.
* Service account-wachtwoorden worden opgeslagen in een wachtwoordkluis met versleuteling en MFA.
* Wachtwoorden moeten direct worden gewijzigd wanneer een medewerker met toegang tot deze accounts de organisatie verlaat.
* Automatische sessies tussen systemen moeten periodiek opnieuw worden geïnitialiseerd, bij voorkeur binnen 24 uur.
* Serviceaccounts met verhoogde privileges worden actief gemonitord op misbruik en afwijkend gedrag.

## Vereisten voor wachtwoordbeheer en -opslag

Ook aan het beheer en de opslag van wachtwoorden zijn eisen verbonden.

**Vereisten**

* Wachtwoorden worden uitsluitend opgeslagen in beveiligde wachtwoordkluizen met versleuteling en MFA.
* Standaard- en universele wachtwoorden mogen niet worden gebruikt.
* Als een systeem een ingebouwd standaard wachtwoord heeft, moet dit na de eerste login worden gewijzigd.
* Er wordt actief monitoring toegepast op wachtwoorden die in openbare datalekken voorkomen.
* Bij vermoedelijk compromitteren van wachtwoorden worden deze onmiddellijk gewijzigd, en de betrokken gebruikers worden geïnformeerd.
* Wachtwoorden van serviceaccounts en accounts met extra rechten worden periodiek gewijzigd en beheerd volgens het vier-ogenprincipe.

# Audit en monitoring van Wachtwoordgebruik

Dit hoofdstuk beschrijft hoe periodieke audits van wachtwoordbeveiliging moeten worden uitgevoerd, evenals het belang van het loggen en monitoren van beheerdersactiviteiten. Het beschrijft ook hoe ongebruikelijke toegangspatronen moeten worden gedetecteerd en hoe beveiligingsincidenten met betrekking tot wachtwoorden moeten worden gerapporteerd en behandeld.

## Periodieke audits van wachtwoordbeveiliging

Met het uitvoeren van regelmatige audits borgen we binnen onze instelling de effectiviteit van het wachtwoordbeleid en het tijdig detecteren van afwijkingen. De audit beoordeelt naleving van de wachtwoordvereisten en identificeert verbeterpunten.

**Vereisten**

* Wachtwoordbeveiligingsaudits worden minimaal jaarlijks uitgevoerd.
* De audit omvat een beoordeling van wachtwoordcomplexiteit, bewaarbeleid en naleving van Multi-Factor Authenticatie (MFA).
* Wachtwoordpraktijken worden vergeleken met actuele dreigingsinformatie en best practices.
* Bevindingen en aanbevelingen worden vastgelegd en opgevolgd binnen een vastgestelde termijn.

## Registratie en bewaking van beheerdersactiviteiten

Het vastleggen en bewaken van activiteiten van beheerdersaccounts is noodzakelijk om ongeautoriseerde wijzigingen en misbruik te detecteren.

**Vereisten**

* Alle aanmeldingen en wachtwoordwijzigingen van beheerdersaccounts worden geregistreerd in een centrale voorziening voor logging en monitoring[[4]](#footnote-5).
* Logs bevatten minimaal: gebruikers-ID, tijdstip, IP-adres en de uitgevoerde actie.
* Loggegevens worden beveiligd opgeslagen en zijn alleen toegankelijk voor geautoriseerd personeel.
* Logs worden minimaal 12 maanden bewaard en periodiek geanalyseerd op afwijkingen.

## Detectie van ongebruikelijke toegangspatronen

Monitoring van inlogpogingen en gebruikersgedrag helpt bij het identificeren van verdachte activiteiten en mogelijke inbraakpogingen.

**Vereisten**

* Inlogpogingen buiten gebruikelijke werkuren of vanaf afwijkende locaties worden gemarkeerd als potentieel verdacht.
* Er wordt gebruikgemaakt van geautomatiseerde detectie van meerdere mislukte aanmeldpogingen binnen een korte tijdspanne.
* Ongebruikelijke wachtwoordwijzigingen worden gedetecteerd en geëvalueerd.
* Als verdacht gedrag wordt vastgesteld, wordt dit automatisch gelogd en geëscaleerd volgens het incidentresponsproces.

## Rapportage van beveiligingsincidenten

Een duidelijk proces voor het melden en afhandelen van wachtwoord gerelateerde incidenten is noodzakelijk om snel en adequaat te reageren op beveiligingsrisico’s.

**Vereisten**

* Beveiligingsincidenten met betrekking tot wachtwoorden worden direct gemeld aan de verantwoordelijke beveiligingsafdeling.
* Incidenten worden vastgelegd in een incidentregistratiesysteem en geclassificeerd op ernst en impact.
* Geautoriseerde medewerkers onderzoeken en documenteren de oorzaak van het incident en bepalen passende mitigerende maatregelen.
* Periodieke rapportages over wachtwoord gerelateerde incidenten worden opgesteld om trends te analyseren en het beleid te verbeteren.

# Opleiding en Bewustwording

De veiligheid van wachtwoorden hangt ook af van de kennis en het gedrag van gebruikers. Dit hoofdstuk behandelt het belang van het trainen van gebruikers over veilige wachtwoordpraktijken, zoals het herkennen van phishing-aanvallen en het belang van wachtwoordcomplexiteit. Het biedt richtlijnen voor het bevorderen van bewustwording over de risico’s van zwakke wachtwoorden en hoe gebruikers ondersteund worden bij het naleven van onze ‘Richtlijn Wachtwoorden’.

## Training en continue bewustwording

Effectieve wachtwoordbeveiliging vereist zowel periodieke training als voortdurende bewustwording onder gebruikers. Door gerichte voorlichting en training houden wij onze gebruikers bewust van best practices en actuele dreigingen.

**Vereisten**

* Alle medewerkers volgen minimaal jaarlijks een training over veilige wachtwoordpraktijken.
* Trainingen behandelen onderwerpen zoals wachtwoordcomplexiteit, veilig opslaan van wachtwoorden en herkennen van phishing-aanvallen en social engineering.
* Medewerkers ontvangen periodieke communicatie over actuele dreigingen en best practices voor wachtwoordbeheer.
* Informatiecampagnes worden ingezet om het belang van unieke en sterke wachtwoorden te benadrukken.
* Gebruikers worden geïnformeerd over de gevaren van hergebruik van wachtwoorden en het belang van Multi-Factor Authenticatie (MFA).
* Medewerkers worden geïnformeerd over veilige wachtwoordbeheertools en de risico’s van ongeoorloofde wachtwoordopslag.

## Wijzigen van zwakke wachtwoorden

Om zwakke wachtwoorden te elimineren, stimuleren wij onze gebruikers hun wachtwoord te wijzigen als het niet voldoet aan de vereisten van deze ‘Richtlijn Wachtwoorden’.

**Vereisten**

* Systemen controleren of wachtwoorden voldoen aan de vastgestelde eisen bij creatie of wijziging.
* Gebruikers ontvangen een melding wanneer hun wachtwoord als zwak wordt geïdentificeerd.
* Wachtwoorden die zijn gelekt in bekende datalekken worden onmiddellijk ongeldig verklaard en moeten door de gebruiker worden gewijzigd.

# Vaststelling

Deze richtlijn is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[FUNTIE].

[Na (her)vaststelling, ook de tabel op p.2 bijwerken]

1. <https://learn.cisecurity.org/cis-password-policy-guide-passphrases-monitoring-and-more> [↑](#footnote-ref-2)
2. <https://sec.surf.nl/bescherm-je-wachtwoorden-effectief-met-een-wachtwoordkluis/> [↑](#footnote-ref-3)
3. Dit kan bijvoorbeeld via een wachtwoordkluis die automatische controle ondersteunt, of door gebruik te maken van een online controletool zoals [haveibeenpwned](https://haveibeenpwned.com/). [↑](#footnote-ref-4)
4. Zie Standaard Logging en Monitoring [↑](#footnote-ref-5)