Wachtwoorden-

beleid (BASIC)

Sjabloon

# Autoriteit en herziening

## Documentcontrole en beoordeling

|  |  |
| --- | --- |
| **Documentcontrole** |  |
| Auteur |  |
| Eigenaar |  |
| Datum aangemaakt |  |
| Laatst herzien door |  |
| Laatste herzieningsdatum |  |

.

## Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum van goedkeuring** | **Goedgekeurd door** | **Beschrijving van verandering** |
| 1.0 |  |  |  |

# Intro

Wachtwoorden worden vaak gebruikt om gebruikers te authentiseren. Dit document biedt een beleid voor het gebruik en de implementatie van wachtwoorden voor vertrouwelijke en kritieke informatiesystemen.

Vroeger dachten we dat de beste manier om wachtwoorden te beveiligen was om ze sterk te maken en vaak te veranderen. Tegenwoordig is wordt de nieuwe filosofie om wachtwoorden lang maar gebruiksvriendelijk te maken steeds populairder. Multi-factor authenticatie wordt sterk aangemoedigd en moet waar mogelijk worden gebruikt, niet alleen voor werk gerelateerde accounts maar ook voor persoonlijke accounts.  
  
Dit beleidsdocument maakt deel uit van een set van beleidsdocumenten die **[Organisatie]** ondersteunen bij het opstellen van een gedegen strategie rond cyberbeveiliging.

# Wachtwoordinstellingen

## Wachtwoordsterkte

De sterkte van wachtwoorden is belangrijk om de kans op misbruik te verkleinen.

Wachtwoordsystemen moeten het gebruik van sterke wachtwoorden afdwingen volgens deze regels:

* De minimaal toegestane lengte van het wachtwoord moet worden aangehouden **(minimaal X tekens, X wordt aanbevolen)**
* Wachtwoorden voor beheerders moeten minimaal **XX** tekens bevatten
* Wachtwoorden voor serviceaccounts moeten minimaal **XX** tekens lang zijn
* Zeer lange wachtwoorden moeten worden toegestaan (bijv. 256 tekens)
* Wachtwoorden die je gebruikersnaam bevatten moeten worden geweigerd
* Wachtwoorden die je voor- of achternaam bevatten moeten worden geweigerd
* Er moeten complexe wachtwoorden worden afgedwongen, die ten minste drie van de volgende categorieën bevatten:
  + - Hoofdletters (A-Z)
    - Kleine letters (a-z)
    - Cijfers (0-9)
    - Speciale tekens: !@#$%^&\*() etc

Uitzonderingen:

In de volgende gevallen is een wachtwoord van minstens 4 cijfers toegestaan:

* Als de code een toevoeging is van een fysieke toegangs-ID zoals een smartcard of token
* Als het systeem niet op een netwerk is aangesloten en sterke fysieke beveiligingscontroles heeft
* Om het scherm van een **[Organisatie]** mobiel toestel zoals een smartphone of tablet te ontgrendelen

## Beleid voor het wijzigen van wachtwoorden

Om het risico op compromitterende wachtwoorden te verkleinen, moeten deze regelmatig worden gewijzigd. De volgende regels zijn van toepassing:

* Standaardwachtwoorden voor nieuwe apparaten moeten worden gewijzigd.
* Systemen moeten gebruikers in staat stellen om wachtwoorden op elk gewenst moment te wijzigen.
* Periodieke verandering van het wachtwoord moet worden afgedwongen, afhankelijk van de afgedwongen minimale wachtwoordlengte van het systeem
* Wanneer de minimaal toegestane wachtwoordlengte van het systeem **X** tekens is, moeten gebruikers worden gedwongen om wachtwoorden elke **X** maanden (of **XX** dagen) te wijzigen.
* Wanneer de minimaal toegestane wachtwoordlengte van het systeem **XX** tekens is, moeten gebruikers worden gedwongen om wachtwoorden elke **X** maanden (of **XX** dagen) te wijzigen.
* Wachtwoorden die zijn verstrekt door anderen dan de gebruiker zelf (bijvoorbeeld de ICT-afdeling) moeten bij de eerste keer inloggen worden gewijzigd.
* Wachtwoordsystemen moeten expliciet het hergebruik van ten minste de laatste **X** wachtwoorden weigeren.
* Gedeelde wachtwoorden die bekend zijn bij mensen die de organisatie verlaten, moeten worden gewijzigd.

Uitzonderingen:

Het beleid om wachtwoorden te wijzigen wordt aanbevolen maar is niet verplicht in de volgende gevallen:

* Als het wachtwoord wordt gebruikt voor een serviceaccount en niet kan worden gebruikt voor interactief aanmelden
* Als de code een toevoeging is van een fysieke toegangs-ID zoals een smartcard of token
* Als het systeem niet op een netwerk is aangesloten en sterke fysieke beveiligingscontroles heeft
* Om het scherm van een **[Organisatie]** mobiel toestel zoals een smartphone of tablet te ontgrendelen

## Preventie van aanvallen

Systemen moeten ten minste één mechanisme hebben om brute force aanvallen te voorkomen. Voorbeelden van dergelijke technieken zijn:

* **accountvergrendeling:**  
  Een uitsluitingsbeleid schakelt de aanmeldfunctionaliteit voor een specifieke account uit. (bijv. Vergrendel account voor **XX** minuten na **X** mislukte aanmeldaccounts).
* **Zwarte IP-lijst**:   
  Net als beleidsregels voor het blokkeren van accounts, detecteert dit mechanisme mislukte aanmeldingen pogingen, maar het controleert van welke IP-adressen de aanmeldingsaanvraag komt. Als er te veel pogingen worden gedetecteerd (bijv. 20) vanaf een bepaald IP-adres, wordt dat adres op de zwarte lijst gezet.
* **Inlogvertraging:**Dit mechanisme voegt een oplopende herhalingsvertraging toe na een verkeerd wachtwoord wordt gebruikt. (bijv. 0,5 seconde wachten na 2 mislukte pogingen, 1 seconde na de derde mislukking, 2 seconden na de vierde, 4 seconden na de vijfde, enz.)

# Wachtwoordbeveiliging

* Wachtwoorden mogen met niemand worden gedeeld, ook niet met supervisors en collega's. Alle wachtwoorden moeten worden behandeld als gevoelige, vertrouwelijke informatie van **[Organisatie]**
* Wachtwoorden mogen niet worden opgenomen in e-mailberichten of andere vormen van elektronische communicatie, of telefonisch aan iemand worden meegedeeld.
* Wachtwoorden mogen alleen worden opgeslagen in wachtwoordmanagers die door de organisatie zijn geautoriseerd. Wachtwoorden op papier moeten worden voorkomen, tenzij er een sterke fysieke beveiliging is (zoals een kluis).
* Gebruik de functie "Wachtwoord onthouden" van toepassingen (bijvoorbeeld webbrowsers) niet.
* Iedereen die vermoedt dat zijn wachtwoord gecompromitteerd is, moet dit melden en alle relevante wachtwoorden wijzigen.

## Distributie via e-mail

Het verspreiden van gebruikersnamen en wachtwoorden via e-mail kan efficiënt en handig zijn. Hoewel e-mail standaard niet het veiligste medium is, kan het worden gebruikt wanneer:

* Er wordt geen extern e-mailsysteem gebruikt.
* E-mail wordt gecodeerd verzonden (zoals Office 365)
* De opgegeven combinatie van gebruikersnaam en wachtwoord verloopt na het eerste gebruik of, indien niet gebruikt, na **1 maand.**

## Distributie via sms

SMS is geen veilig protocol en mag nooit gebruikt worden om gebruikersnaam- en wachtwoordcombinaties te versturen. Het kan worden gebruikt voor het verzenden van gedeeltelijke aanmeldingsinformatie, maar alleen als aan de volgende voorwaarden wordt voldaan:

* Het bericht bevat maximaal slechts één deel van de combinatie: systeem, gebruikersnaam, wachtwoord of token. De andere delen worden via andere distributiemethoden verzonden.
* De gebruiker verwacht het bericht en zal het daarom waarschijnlijk binnenkort gebruiken.
* De informatie in het bericht verloopt na het eerste gebruik of, als het niet wordt gebruikt, na 1 maand.