

Wachtwoorden- en authenticatiebeleid gemeente Aa en Hunze

1. Algemene beleidsuitgangspunten

De doelstelling van dit wachtwoorden- en authenticatiebeleid van de gemeente Aa en Hunze is het voorkomen van onbevoegde toegang tot systemen en toepassingen door:

- Het vaststellen van regels waar wachtwoorden en wachtwoord procedures aan moeten voldoen.
- Het vaststellen van de bescherming van de wachtwoorden.
- Het vaststellen van de wijzigingscriteria voor wachtwoorden.
- Het definiëren van authenticatie tot geclassificeerde informatiesystemen.

Dit wachtwoorden- en authenticatiebeleid van de gemeente Aa en Hunze voldoet aan de wachtwoordvereisten vanuit de Baseline Informatiebeveiliging Overheid (BIO). De gemeente Aa en Hunze hanteert het volgende wachtwoorden- en authenticatiebeleid in de praktijk.

1.1 Wachtwoorden

Ten aanzien van wachtwoorden geldt tenminste:

- Standaard wachtwoorden, die in systemen zitten (leveranciers), worden voor ingebruikname gewijzigd.
- Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd.
- Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker).
- 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 1 werkdag geldig.
- Wachtwoorden zijn alleen bij de gebruiker bekend.
- Wachtwoorden dienen de complexiteitseisen vanuit de BIO te volgen.
- Wachtwoorden zijn maximaal een jaar geldig indien de (informatie)-systemen voldoen aan het wachtwoord beleid. Anders zijn de wachtwoorden maximaal 6 maanden geldig.
- Wachtwoorden mogen niet herhaaldelijk worden gebruikt.
- Om risico's te verminderen, kunnen wachtwoordeisen ad hoc worden gewijzigd.

1.1.1. Basis voor wachtwoordbeleid. De basis voor dit wachtwoordenbeleid is de actuele 'Active Directory domain policy' (AD) van de gemeente Aa en Hunze (11-05-2021) en voldoet aan de BIO. Deze policy is de basis voor de VDI werkplek, het Mobile Device Management en de Microsoft Office 365 omgeving. Onderstaand is de kern hiervan weergegeven:

Policy	Policy Setting
 Enforce password history	20 passwords remembered
 Maximum password age	90 days
 Minimum password age	0 days
 Minimum password length	8 characters
 Minimum password length audit	Not Defined
 Password must meet complexity requirements	Enabled
 Store passwords using reversible encryption	Disabled

Voor toegang tot computers, zoals smartphones en laptops, van de gemeente Aa en Hunze geldt een pincode van 6 cijfers.

1.1.2 Verlopen van een wachtwoord. Voordat een AD wachtwoord verloopt krijgen gebruikers 4 keer een waarschuwingsmail. Om de maand worden accounts die al langer dan een maand niet zijn ingelogd geanalyseerd, besproken met de teamleider en eventueel buiten gebruik gesteld. Verlopen wachtwoorden worden door de servicedesk of, bij een specifieke applicatie, via de functioneel beheerder gereset. Bij verlopen AD wachtwoorden wordt een tijdelijk nieuw wachtwoord uitgegeven door de servicedesk.

1.1.3 Opslag van wachtwoorden. Volgens de BIO dienen gebruikers ondersteund te worden in het beheer van hun wachtwoorden door het beschikbaar stellen van een wachtwoordkluis door de gemeente Aa en Hunze. De gemeente Aa en Hunze biedt medewerkers de wachtwoordkluis van KeePass aan.

1.2 Authenticatie

Authenticatie gaat om het vaststellen van de identiteit van de medewerker die een inlogpoging doet. Ten aanzien van authenticatie geldt:

- Toegang tot geclassificeerde informatiesystemen van de gemeente Aa en Hunze vindt plaats op basis van een wachtwoord en multi-factor authenticatie (MFA).
- Standaard geldt twee-factor authenticatie (2FA) om toegang te krijgen tot de werkplek met taak specifieke applicaties, de Microsoft Azure omgeving en de Microsoft Office 365 omgeving.
- De schermbeveiliging, de 'screen-lock', kan met een wachtwoord worden opgeheven. Als er een 'lock-out' (max. 12 uur) optreedt dient er opnieuw met 2FA ingelogd te worden.
- Er wordt gestuurd op Single Sign On (SSO), met als basis de Azure Active Directory (Azure AD).

1.2.1 Multi-factor authenticatie. Afhankelijk van het risico en het daarbij behorende beveiligingsniveau, kunnen aanvullende authenticatie factoren ingezet worden. Er is dan sprake van 'multi-factor authenticatie' (MFA). Bij deze factoren valt te denken aan tokens, het 'aanwezig zijn in een bepaalde ruimte' (het gemeentehuis) of een geïnstalleerd certificaat. De gemeente Aa en Hunze heeft twee mogelijke werksituaties:

Op werklocaties van de gemeente Aa en Hunze:

- 1^e) gebruikersnaam en wachtwoord
- 2^e) locatie (gemeentehuis)

Buiten werklocaties van de gemeente Aa en Hunze:

- 1^e) gebruikersnaam en wachtwoord
- 2^e) token (Microsoft Authenticator app)

1.3 Rapportage en controle

Functioneel beheerders (uit naam van de teamleiders; de eigenaren) controleren aantoonbaar minimaal eens per jaar of de wachtwoordvereisten en authenticatie van medewerkers nog juist zijn.

Dit is een geactualiseerde versie van het huidige wachtwoordenbeleid (ISMS 11.2.3 op het wachtwoordenbeleid van 2019) en treedt in werking na vaststelling door de gemeentesecretaris. Hiermee komen eerdere versies van het wachtwoordenbeleid van de gemeente Aa en Hunze te vervallen.

Aldus vastgesteld door Marleen Tent, gemeentesecretaris:

A blue ink signature of Marleen Tent, consisting of several overlapping loops and a horizontal line at the bottom.

Handtekening

24 juni 2021

Datum