Gemeente
EDAM
VOLENDAM

Informatiebeveiliging

Gemeente Edam-Volendam

Wachtwoordbeleid

26 februari 2020
Versie 1.0

Auteur:
C.A. Sneekes, CISO

Beleidsuitgangspunten voor het gebruik van wachtwoorden

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.

Het wachtwoordbeleid is onderdeel van het informatiebeveiligingsbeleid van de gemeente Edam-Volendam en een aanvulling op het Strategisch Informatiebeveiligingsbeleid Gemeente Edam-Volendam 2020-2023. Het wachtwoordbeleid is in lijn met de Baseline Informatiebeveiliging Overheid (BIO) en voldoet aan de wettelijke regelgevingen en beleidsdocumenten van gemeente Edam-Volendam.

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.

De gemeente Edam-Volendam hanteert de volgende beleidsuitgangspunten en deze zijn ontleend aan de Baseline Informatiebeveiliging Overheid (BIO).

Algemeen beleid

1. Toegang tot besturingssystemen van de gemeente wordt beheerst met een beveiligde inlogprocedure.
2. Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
3. Wachtwoorden worden op een veilige manier uitgegeven op basis van een formele registratie- en afmeldingsprocedure.
4. Gebruikers bevestigen de ontvangst van een wachtwoord.
5. Tijdelijke wachtwoorden, wachtwoorden die gereset zijn en initiële wachtwoorden hebben een geldigheidsduur van maximaal 24 uur en moeten bij het eerste gebruik worden gewijzigd.
6. Standaard wachtwoorden, die in systemen zitten, worden voor ingebruikname gewijzigd.
7. Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
8. Waar mogelijk wordt er gebruik gemaakt van Single-signon.
9. Toegang tot externe kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.
10. Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.

Wachtwoordgebruik

11. Gebruikers behoren goede beveiligingsgewoonten in acht te nemen bij het kiezen en gebruiken van wachtwoorden.

12. Aan de gebruikers wordt een set gedragsregels aangereikt met daarin minimaal het volgende:
    a. Wachtwoorden worden niet opgeschreven.
    b. Gebruikers delen hun wachtwoord nooit met anderen.
    c. Wachtwoorden mogen niet opeenvolgend zijn.
    d. Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde.
    e. Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro).
    f. Misbruik van wachtwoorden dient als beveiligingsincident gemeld te worden aan de servicedesk en/of CISO.
13. Nadat voor een gebruikersnaam vijf 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 resetten volgens de geldende procedure.
14. Wachtwoorden dienen te bestaan uit minimaal 20 karakters. Indien informatiesystemen dit niet toelaten, mag voor een verkort wachtwoord (minimaal 10 karakters) gekozen worden, waarbij minimaal gebruik gemaakt wordt van drie van de vier verschillende karaktersets: hoofdletters, kleine letters, cijfers en/of speciaal karakters.
15. Wachtwoorden zijn maximaal een jaar geldig indien de (informatie)-systemen voldoen aan het wachtwoord beleid. Anders zijn de wachtwoorden maximaal 3 maanden geldig.
16. Het aantal foutieve inlogpogingen staat op maximaal 5x, daarna wordt het account (tijdelijk) geblokkeerd.

Wachtwoordbeheer

17. Systemen voor wachtwoordbeheer zijn interactief en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.
18. Gebruikers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.
19. Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).
20. Wanneer het wachtwoord is verlopen, wordt het account geblokkeerd.
21. Wachtwoorden worden versleuteld opgeslagen of verstuurd, maar nooit in originele vorm (plaintext).
22. De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthentiseerd.

Aldus vastgesteld door de portefeuillehouder Informatiebeveiliging van gemeente Edam-Volendam

op 5-3-2020,

H. van der Woude
Gemeentesecretaris

L.J. Sievers
Burgemeester