Beleid wachtwoorden en tweestapsverificatie
Onderwijsgroep Amersfoort

Versiebeheer

Versienr.	Datum	Auteur	Akkoord	Wijzigingen
1.0	27-09-2018	Gert-Jan de Leeuw		Initiële versie wachtwoordbeleid
2.0	19-11-2021	John Storms		Update beleid naar geldende marktstandaarden.

Inhoudsopgave

1. Inleiding 3
2. Algemeen Beleid 4
3. Wachtwoorden van alle medewerkers en leerlingen 4
4. Aanvullend wachtwoordbeleid beheerders 5
5. Wachtwoordbeheer 5
6. Wachtwoorden mobiele apparaten 5
7. Wachtwoorden WiFi 6
8. Tweestapsverificatie 6
9. Encryptie 6
10. Tips voor verzinnen van veilige wachtwoorden 7
11. Rapportage en Controle 7

1. Inleiding

Ten behoeve van de beveiliging van informatie binnen de Onderwijsgroep Amersfoort is dit beleid er op gericht om een richtlijn te geven hoe er binnen de scholengemeenschap omgegaan moet worden met wachtwoorden en tweestapsverificatie. Wachtwoorden en tweestapsverificatie zorgen ervoor dat onbevoegden geen toegang kunnen krijgen tot de informatie van Onderwijsgroep Amersfoort. Een gemakkelijk wachtwoord evenals onduidelijke of niet gevolgde wachtwoord procedures zijn niet alleen een bedreiging voor de vertrouwelijkheid en integriteit van de informatie, maar uiteindelijk ook slecht voor het imago van de onderwijsgroep. Alle gebruikers van informatiesystemen dienen goede wachtwoorden te kiezen en zijn verantwoordelijk voor de geheimhouding van hun wachtwoorden en login-gegevens.

Het doel van dit beleid is vierledig:

- Het vaststellen van regels waar wachtwoorden en wachtwoord procedures aan moeten voldoen.
- Het vaststellen van de bescherming van wachtwoorden.
- Het vaststellen van de wijzigingscriteria voor wachtwoorden.
- Het vaststellen van het aanvullend gebruik van tweestapsverificatie.

2. Algemeen Beleid

Binnen de Onderwijsgroep Amersfoort zijn er richtlijnen vastgelegd omtrent de wachtwoorden en gebruik daarvan. De volgende regels gelden voor de medewerkers:

- Standaard wachtwoorden, die in systemen zitten, worden voor ingebruikname gewijzigd.
- Wachtwoorden worden nooit in plaintext opgeslagen, maar in plaats daarvan met encryptie.
- Wachtwoorden worden nooit in combinatie met een gebruikersnaam verstuurd.
- Wachtwoorden worden nooit op dezelfde wijze verstuurd als de gebruikersnamen (E-mail, SMS of whatsapp).
- De systeembeheerder dient goedkeuring te krijgen van een aangewezen persoon voor het resetten van een medewerkers wachtwoord. De goedkeuring kan verstrekt worden per mail of een bekend telefoonnummer.
- Ten aanzien van wachtwoorden gelden de volgende regels:
    - Wachtwoorden worden op een veilige manier uitgegeven d.m.v. controle door de contactpersoon en tekenbevoegde.
    - Tijdelijke wachtwoorden of wachtwoorden die standaard in software of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord.
    - Gebruikers bevestigen ontvangst van een wachtwoord.
    - Wachtwoorden zijn alleen bij de gebruiker bekend.
    - Wachtwoorden bestaan uit minimaal 10 vrij te kiezen karakters, waarvan tenminste 1 kleine letter, 1 hoofdletter, 1 cijfer en 1 teken.
    - Wachtwoorden zijn maximaal 180 dagen geldig en mogen niet binnen 20 keer herhaald worden.

De regels gelden voor toegang tot alle omgevingen (Windows, Google) en applicaties van Onderwijsgroep Amersfoort en de daaronder vallende scholen. De regels zijn verplicht voor alle medewerkers en worden aanbevolen voor leerlingen.

3. Wachtwoorden van alle medewerkers en leerlingen

Medewerkers behoren goede beveiligingsgewoonten in acht te nemen bij het kiezen en gebruiken van wachtwoorden. Aan de gebruikers worden de volgende gedragsregels aangereikt:

- Wachtwoorden worden niet opgeschreven.
- Gebruikers delen hun wachtwoord niet 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 beheerders.
- Na 7 foutieve aanmeldpogingen wordt het account geblokkeerd en dient deze door de systeembeheerder weer geactiveerd te worden.

De bovengenoemde beveiligingsgewoonten zijn verplicht voor alle medewerkers en worden aanbevolen voor alle leerlingen.

4. Aanvullend wachtwoordbeleid beheerders

Toegang tot besturingssystemen, applicaties en servers behoort te worden beheerst met een beveiligde inlogprocedure.

- Administrator wachtwoorden worden bewaard in een wachtwoorddatabase met encryptie.
- Ten aanzien van wachtwoorden gelden de volgende regels:
    - Wachtwoorden bestaan uit minimaal 10 vrij te kiezen karakters, waarvan tenminste 1 kleine letter, 1 hoofdletter, 1 cijfer en 1 vreemd teken.
    - Wachtwoorden zijn maximaal 240 dagen geldig en mogen niet binnen 20 keer herhaald worden. Met enkele uitzonderingen voor service wachtwoorden.
- De standaard wachtwoorden van nieuwe apparatuur dienen bij aanvang gewijzigd te worden. Denk bijvoorbeeld aan printers, switches, NAS, server etc.

De beheerders wordt daarnaast ook geadviseerd om het wachtwoordbeleid zoveel mogelijk, voor de medewerkers, systeembeheerders en applicatiebeheerders technisch af te dwingen.

5. Wachtwoordbeheer

Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

- De systeembeheerder dient ervoor te zorgen dat het wachtwoord beleid, waar mogelijk, technisch wordt afgedwongen aan de medewerkers.
- Wachtwoorden hebben een maximale geldigheidsduur zoals vermeld in hoofdstuk 2. Binnen deze tijd dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.
- Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.
- Een medewerker heeft de mogelijkheid om het eigen wachtwoord te wijzigen. Hiervoor geld dat de medewerker geauthentiseerd moet zijn, voordat het wachtwoord gewijzigd kan worden.

6. Wachtwoorden mobiele apparaten

Meerdere medewerkers hebben in verband met hun functie een mobiele telefoon of een tablet waarop ook informatie kan staan (denk aan de e-mail). Deze apparaten dienen beveiligd te worden met de volgende authenticatie mogelijkheden:

- Vingerafdruk
- Gezichtsscan
- Minimaal 6-cijferig pincode

De pincode mag niet eenvoudig te raden zijn zoals “000000” of “123456”.

7. Wachtwoorden WiFi

Het WiFi is een belangrijk toegangspunt tot het netwerk. Het is hierom nodig om ook dit wachtwoord periodiek te wijzigen. Voor het wijzigen van de WiFi wachtwoorden worden de onderstaande regels gehanteerd. Op alle client apparaten dient het nieuwe wachtwoord opgegeven te worden.

- Het WiFi wachtwoord t.b.v. het kantoor netwerk wordt elke 240 dagen gewijzigd.
- Het WiFi wachtwoord t.b.v. het gasten netwerk wordt elke 240 dagen gewijzigd.

8. Tweestapsverificatie

Tweestapsverificatie is een extra beveiligingscontrole voor het inloggen op een netwerk, applicaties of cloud diensten. Het gebruik van een tweestapsverificatie is verplicht voor alle medewerkers van Onderwijsgroep Amersfoort en wordt aanbevolen voor alle leerlingen van de scholen van Onderwijsgroep Amersfoort waar de toepassing dit mogelijk maakt. Hierbij dient rekening gehouden te worden met het volgende:

- De tweestapsverificatie op cloud diensten zoals MS Office 365 en Google Workspace wordt ingeschakeld voor alle medewerkers.
- De tweestapsverificatie op cloud diensten zoals MS Officer 365 en Google Workspace wordt aanbevolen voor alle leerlingen.
- De tweestapsverificatie wordt ingeschakeld voor alle medewerkers die inloggen externe applicaties waar privacy gevoelige informatie wordt opgeslagen.
- De tweestapsverificatie wordt ingeschakeld voor alle medewerkers die remote verbinding maken met het kantoor/school netwerk.

9. Encryptie

Voor de medewerkers die gebruik maken van een laptop is het gebruik van encryptie van de hard schijf verplicht, bijvoorbeeld via Bitlocker (Microsoft) of alternatieven. Bitlocker zorgt ervoor dat de laptop harde schijven encrypted zijn. In het geval van verlies of diefstal is het bijna niet mogelijk om gegevens van de laptop in te zien. Bij het activeren van bitlocker dient er rekening gehouden te worden met het volgende:

- Bitlocker wordt door de systeembeheerder afgedwongen.
- De systeembeheerders bewaren de Bitlocker herstel-codes.

Het gebruik van Bitlocker of alternatieven wordt aanbevolen voor leerlingen.

10. Tips voor verzinnen van veilige wachtwoorden

Het is steeds moeilijker om een wachtwoord te bedenken dat zowel veilig als makkelijk te onthouden is. Door woorden, zinnen en getallen te combineren en ze te coderen met wat eenvoudige aanpassingen weet je zeker dat de informatie veilig is. De volgende tips kunnen erbij helpen om een moeilijk wachtwoord te maken en toch deze eenvoudig te onthouden.

- **Maak een samengesteld woord.** Combineer drie of meer woorden die iets voor je betekenen. Vervang de eerste of laatste letter van elk woord door een hoofdletter. Voeg als laatste cijfers of symbolen toe. Dit mag ook door bepaalde letters daarnaartoe aan te passen.
  Voorbeeld: school werk salaris → Sch00lWerkS@l@ris
- **Verbind de eerste letters van een zin.** Combineer de eerste letters van een zin die makkelijk te onthouden is**.** Vervang klinkers door symbolen of cijfers of voeg deze toe.
  Voorbeeld: wij werken op een school in de stad amersfoort → wW03S1ds@
- **Bedenk een wachtwoord zin.** Een lang wachtwoord is soms veiliger dan een kort moeilijk wachtwoord. Bedenk een zin die makkelijk te onthouden is, voeg tekens en cijfers toe en gebruik dit als wachtwoord.
  Voorbeeld: W$rken0nderwijsgroepAmersf00rt
- **Neem een woord of zin en vervang de klinkers.** Kies een persoonlijke woord of zin die andere niet makkelijk kunnen raden. Vervang daarvan alle klinkers door cijfers of symbolen.
  Voorbeeld: AmersfoortGroep → @m3rsf00rtGr03p

11. Rapportage en Controle

Er vindt controle plaats op het wachtwoord gebruik en bij eventuele incidenten wordt er gerapporteerd.

- De systeembeheerder rapporteert eventuele incidenten aan de directie of de verantwoordelijke.
- De systeembeheerders monitoren servers en cloud omgevingen op foutieve inlog pogingen.
- De systeembeheerder controleert of het wachtwoordbeleid technisch is doorgevoerd voor alle medewerkers.

12. Tot slot

Indien er vragen zijn over dit beleid van Onderwijsgroep Amersfoort of de toepassing daarvan kan contact opgenomen worden met de privacy coördinator van de school of een mail gestuurd worden naar: privacy@onderwijsgroepamersfoort.nl. Het beleid wordt tenminste elke 2 jaar geüpdatet en is voor het laatst aangepast per 7 december 2021.