WACHTWOORDBELEID

vzw VRIJ KATHOLIEK BASISONDERWIJS DE WEGWIJZER

voor:

VRIJ KATHOLIEK BASISONDERWIJS DE WEGWIJZER bestaande uit de scholen:

- **VBS Beveren-Leie**
- **VBS Biest-Jager**
- **VBS Desselgem**
- **VBS Duizend+Poot**
- **VBS Gaverke-College**
- **VBS Keukeldam – Sint-Petrus**
- **VBS Nieuwenhove**
- **VBS Zulte**

Deze nota maakt deel uit van het informatieveiligheids- en privacybeleid (IVPB).

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2019-01-22	GELDIG	CIV	

Inhoud

1. INLEIDING

Een goed beveiligingsbeleid is tegenwoordig noodzakelijk voor elke school. Steeds meer privacygevoelige gegevens worden (online) gedeeld en een zwak beveiligingsbeleid zorgt ervoor dat je de deur openzet voor duidelijke risico's. Een goed beveiligingsbeleid geeft gebruikers (leerkrachten, leerlingen, CLB-medewerkers…) toegang tot alle informatie die ze nodig hebben om hun taak naar behoren uit te oefenen maar ontzegt hen alle toegang tot informatie die ze niet nodig hebben.

Er zijn drie pijlers waarop een goed beveiligingsbeleid berust: **authenticatie, autorisatie en auditing**.

Authenticatie is het proces waarbij je je identiteit gaat bewijzen (ben je wel diegene die je beweert te zijn). Vaak doen we dit door combinatie van een gebruikersnaam en een wachtwoord.

Autorisatie is een proces waarbij onderzocht wordt of je voldoende rechten hebt of toestemming hebt voor hetgeen je wilt doen. Bijvoorbeeld: een leerkracht zal toestemming hebben om in het puntenboek van de klas te schrijven, de leerling mag alleen zijn eigen punten lezen. Enkel de zorgverantwoordelijke en de directie kan in het zorgdossier van een leerling schrijven.

Auditing (Controleerbaarheid) is het proces waarmee je kan nagaan wie wat waar, wanneer en waarmee doet. Vaak heb je hiervoor een hulpmiddel nodig dat je kan vertellen wat er op elk moment gebeurde. Dit kan onder meer in de vorm van een logboek.

In dit document zullen we ons beperken tot de authenticatie en in het bijzonder het gebruik van wachtwoorden en andere, bijkomende authenticatiemethodes op Vrij Katholiek Basisonderwijs De Wegwijzer.

Deze nota valt onder de eindverantwoordelijkheid van vzw Vrij Katholiek Basisonderwijs De Wegwijzer.

2. TOEGANGSBEHEER

De coördinerend directeur van de scholengemeenschap is verantwoordelijk voor het gebruikersbeheer van de organisatie. Gebruikersbeheer houdt het aanmaken van gebruikers, toekennen van rechten en stopzetten van rechten in. Dit betekent dat er in de scholengemeenschap een inventaris moet opgezet worden die het overzicht houdt van alle rollen en rechten gekoppeld aan personeelsleden in de scholengemeenschap. Het opzetten van een dergelijke procedure rond het toegangsbeheer is belangrijk om de controle te kunnen houden op alle gebruikers die er zijn in de organisatie. Dit is de eerste stap in het authenticatiebeleid.

3. AUTHENTICEREN

Er zijn verschillende manieren om je in systemen te authenticeren. De meest gebruikte vorm is de combinatie van een gebruikersnaam en een wachtwoord. Een ander voorbeeld is het gebruik van je bankkaart en je pincode waarmee je je aan een bankautomaat kan authenticeren. Maar ook een vingerafdruk of een irisscan kan gebruikt worden om te kijken of je wel diegene bent die je beweert te zijn.

Wachtwoorden zorgen er mee voor dat de toegang tot applicaties goed beveiligd is. Het is dus van belang om een sterk beleid op te zetten om het inlogproces en -procedures te beheren. Op Vrij Katholiek Basisonderwijs De Wegwijzer werken we er continu aan om leerkrachten en leerlingen het belang van sterke wachtwoorden bij te brengen.

Een wachtwoordbeleid heeft als doel enkele bepalingen op te leggen rond het correct gebruik van wachtwoorden om de toegang tot gevoelige data (waaronder privacy gevoelige persoonsgegevens) te beveiligen middels een wachtwoord.

Een sterk wachtwoord is moeilijker te achterhalen en dus veiliger dan een ‘zwak’ wachtwoord. De sterkte van een wachtwoord hangt af van de lengte, complexiteit en de onvoorspelbaarheid.

3.1. Wachtwoordbepalingen

Voor zijn wachtwoordbeleid volgt Vrij Katholiek Basisonderwijs De Wegwijzer de aanbevelingen/vereisten van Microsoft voor Office 365.

- Het wachtwoord moet bestaan uit minstens 8 en maximaal 16 karakters.
- Het moet bestaan uit minstens 3 van de 4 volgende tekens:
  - Hoofdletters
  - Kleine Letters
  - Cijfers
  - Niet-alfanumerieke tekens: @ # $ % ^ & * - _ ! + = [ ] { } | \ : ‘ , . ? / ` ~ “ ( ) ;
- Beter nog is om te werken met een wachtwoordzin (bijv: IkHeb2Kinderen)
- Gebruik de hoofdletters en andere karakters best niet in het begin van het wachtwoord/wachtzin en wissel ze met elkaar af. Bijv. p@dd€NSto€l579
- Keer woorden om. Bijv. l€otSN€dd@p579
- Maak wachtwoorden/wachtzinnen die enkel betekenis hebben voor jou.
- Verander minstens één keer per schooljaar je wachtwoord.
- Gebruik verschillende wachtwoorden voor verschillende applicaties; hergebruik je wachtwoord niet!

Gebruik een online tool om te zien hoe sterk jouw wachtwoord is: bijv. https://veiliginternetten.nl/wachtwoord-check

3.2. Afraders

- Gebruik geen voor de hand liggende namen, woorden of getallen.
  Bijv. NaamVoornaamGeboortedatum of StraatnaamNr
- Schrijf het wachtwoord niet op: niet op papier, niet elektronisch in jouw GSM of PC. Bewaar ze zeker niet op een Post-it aan de computer.
  - ❖ Indien je toch liefst je wachtwoord opschrijft, bewaar het dan ver van de gebruiker en schrijf er niet bij voor welke applicatie het dient.
- Geef het wachtwoord niet door, op geen enkele wijze aan niemand.
- Verzend nooit een wachtwoord via email of een ander communicatiesysteem. (Niemand van Vrij Katholiek Basisonderwijs De Wegwijzer zal ooit je wachtwoord, om eender welke reden, op deze manier opvragen.)
- Zorg dat niemand op je vingers kijkt bij het ingeven van een wachtwoord.
- Er is soms de optie om een wachtwoord (even) te tonen, zodat je typfouten kan controleren. Zorg dat er niemand meekijkt op het moment dat je dit gebruikt.
- Besteed bijzondere aandacht aan een externe projectie indien dat aangesloten is, zoals bv. een beamer of (groot) tweede scherm.
- Gebruik geen woord uit het woordenboek.
- Herhaal niet te veel karakters of nummers (bijv. 11223344).
- Gebruik geen te makkelijke wachtwoorden (bijv. NaamAchternaamGeboortejaar, azertyuiop).
- Bewaar je wachtwoord niet in de browser.
- Maak geen gebruik van de functie om ingelogd te blijven in een bepaalde applicatie.
- Gebruik andere wachtwoorden dan privé-wachtwoorden.

3.3. Wachtwoordbeheer

- Na 10 pogingen om in te loggen wordt het account vergrendeld. Neem contact op met de dienst ICT om het account terug te ontgrendelen.
- Laat de computer nooit onbeheerd achter maar vergrendel het scherm of log uit.
- Na x minuten inactiviteit valt de computer automatisch in slaapmodus en wordt het scherm vergrendeld.
- Er wordt automatisch gecontroleerd op het gebruik van goede wachtwoorden.
- De wachtwoorden van de personeelsleden zijn in het bezit van de systeembeheerder en de ICT-co's met als doel toestellen te kunnen configureren voor de gebruikers / tussen te kunnen komen bij problemen. De systeembeheerder/ICT-co gaat hier zeer discreet en professioneel mee om. Geenszins dient dit om persoonlijke gegevens, e-mail, etc. van het personeelslid te bekijken.

3.4. Wat doen bij vermoeden van misbruik?

Misbruik kan ontvreemding of onrechtmatig gebruik van een wachtwoord zijn.

Neem direct contact op met het aanspreekpunt informatieveiligheid, de dienst ICT en/of de systeembeheerder. Meldpunt datalekken: privacy@ko-dewegwijzer.be

Deze personen gaan na of er sprake is van een misbruik en proberen zo nodig de schade te herstellen.

3.5. Wat doen indien het wachtwoord vergeten werd

- Blijf niet proberen; na een aantal pogingen zal je account vergrendeld worden (zie § 3.3)
- Anders neem je persoonlijk contact op met de dienst ICT en/of de systeembeheerder. Zij zullen een nieuw wachtwoord instellen (d.i. een “wachtwoordreset”) waarmee de gebruiker terug kan aanmelden.

3.6. Gebruik van wachtwoordmanagers of een wachtwoordkluis

Indien je te veel wachtwoorden moet onthouden, kan je gebruik maken van een wachtwoordkluis. Wachtwoordkluizen slaan al de wachtwoorden versleuteld op in een beveiligd bestand. Dit bestand wordt geopend met één sterk wachtwoord. Dit wil zeggen dat er maar één wachtwoord meer nodig is om alle wachtwoorden veilig te ontsleutelen.

De volgende wachtwoordkluizen werden veilig bevonden voor onze scholengemeenschap:

- KeePass (http://keepass.info/)
- LastPass (https://lastpass.com/nl/)
- Dashlane (https://www.dashlane.com/)
- Password (https://agilebits.com/onepassword)
- Passwordsafe (https://www.pwsafe.net/)

4. GEBRUIK VAN TWO-FACTOR AUTHENTICATIE

Indien je echt met veel privacygevoelige persoonsgegevens werkt, is vaak een combinatie van gebruikersnaam en wachtwoord niet voldoende veilig. De gebruikersnaam is meestal gekend en een wachtwoord kan eventueel gestolen of ontfutseld worden. Daarom bestaan er two-factor authenticatiemethodes.

Een voorbeeld: Naast het gebruik van een gebruikersnaam en wachtwoord krijg je op je gsm een beveiligingscode doorgestuurd die je dan extra moet ingeven vooraleer je toegang krijgt. Naast het weten van de gebruikersnaam en wachtwoord is het dus ook nodig dat je iets in je bezit hebt, zoals bijvoorbeeld een telefoon waar men via sms een code doorgestuurd krijgt.

Deze systemen zijn veel veiliger en worden binnen Vrij Katholiek Basisonderwijs De Wegwijzer dan ook toegepast voor iedereen die aan de meest privacygevoelige gegevens binnen de onderwijsinstelling kan. Concreet denken we hierbij aan iedereen die toegang heeft tot geheime gegevens (zie classificatie van gegevens en de toegangsmatrices).

5. RISICO'S

Aan een slecht wachtwoordbeleid zijn risico's verbonden. Met dit beleid willen we onderstaande risico's verkleinen en/of uitschakelen.

- **Identiteitsdiefstal**: iemand die jouw wachtwoord achterhaalt, kan zich binnen de systemen in kwestie voordoen met jouw identiteit. Alle handelingen die men met jouw account stelt, worden via logging teruggebracht naar uzelf en niet naar diegene die met uw digitale identiteit aan de haal ging.
- **Phishing**: via phishing proberen oplichters achter persoonlijke gegevens/wachtwoorden te komen, meestal via e-mail of telefoon. Met deze informatie kunnen oplichters persoonlijke gegevens stelen en publiceren.

  Zie **Achtergrondinformatie** – § 1 voor meer informatie rond "phishing".

- **Hacking**: door zwakke wachtwoorden wordt het zeer eenvoudig om in te breken in de informatiesystemen. Eens binnen in het systeem kan er zeer veel schade berokkend en kunnen gegevens gestolen worden.

Rond deze risico's worden alle personeelsleden, maar zeker ook de leerlingen en ouders, binnen Vrij Katholiek Basisonderwijs De Wegwijzer actief en herhaaldelijk gesensibiliseerd.

O.a. via Safe on Web kan er veel praktisch materiaal gevonden worden rond dit beleid en rond de hier vermelde risico's:

https://www.safeonweb.be/nl/home