Hellingstraat 44
1800 Vilvoorde
Tel 02 257 10 49
info@kov.be www.kov.be

Wachtwoordbeleid

KOV vzw

Met volgende instellingen:

Basisonderwijs:

De Biekorf

De Knipoog

De Lampion

Heilig-Hartschool

Sint-Jozef Groenstraat

De Windroos

Parochiale Basisschool Diegem

Buitengewoon lager onderwijs:

Klavertje Vier

Secundair onderwijs:

Het College

TechnOV

Virgo Plus

Topsportinternaat volleybal

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

Aangemaakt: 10/09/2021 - Laatst aangepast: 9/10/2023 - Document revisienummer: 8

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 direct bij het kind betrokken verantwoordelijken kunnen in de verschillende dossiers van de desbetreffende leerling lezen/schrijven, al naar gelang hun bevoegdheid.

***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 KOV vzw.

Deze nota valt onder de eindverantwoordelijkheid van KOV vzw.

2 Toegangsbeheer

De inrichtende macht heeft de eindverantwoordelijk over het beleid rond gebruikersbeheer van de organisatie. Gebruikersbeheer wordt, na het ondertekenen van een deontologische code, uitgevoerd door de ICT-coördinatoren en houdt het aanmaken van gebruikers, toekennen van rechten en stopzetten van rechten in. Dit betekent dat er in de school een inventaris moet opgezet worden die het overzicht houdt van alle rollen en rechten gekoppeld aan personeelsleden in de school. 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

Wachtwoorden zorgen er mee voor dat de toegang tot applicaties zo goed mogelijk beveiligd is. Het is dus van belang om een sterk beleid op te zetten om het inlogproces en -procedures te beheren. Op KOV vzw 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 privacygevoelige 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.

Voor personeelsleden die met grote waarschijnlijkheid vertrouwelijke informatie verwerken/delen via email wordt op mobiele toestellen een mobile device policy geïnstalleerd op elk van hun mobiele toestellen.

- Pincode minimaal 4 tekens is verplicht
- Informatie die binnenkomt wanneer schermvergrendeling is ingeschakeld wordt verborgen (optioneel, maar wel aan te raden)

3.1 Wachtwoordbepalingen

- Hoe langer een wachtwoord hoe beter. Het wachtwoord moet minstens 8 karakters hebben. Beter nog is om te werken met een wachtwoordzin (bijv: Igs2015NdS -> `IkGaSinds2015NaarDeSchool`)
- Mix hoofdletters, kleine letters en tekens door elkaar: gebruik volgende tekens in het wachtwoord:
  - Hoofdletters
  - Kleine letters
  - Cijfers
  - Niet-alfanumerieke karakters

  Bijv. `P@dd€nsto€l579`

- 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.
- Veranderen van het wachtwoord wordt minstens één keer per semester afgedwongen.
- Gebruik verschillende wachtwoorden voor verschillende applicaties; hergebruik je wachtwoord niet!
- Indien de ICT-dienst een wachtwoord instelt of “reset” (zie ook § 3.5) voor een bepaald platform of voor het netwerk, dan zal de gebruiker dit steeds moeten veranderen naar een persoonlijk wachtwoord, bij de eerste aanmelding.

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.
- Geef het wachtwoord niet door, op geen enkele wijze aan niemand (ook niet aan iemand van ICT).
- Verzend nooit een wachtwoord via email of een ander communicatiesysteem. (Niemand van KOV vzw 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

- Laat de computer nooit onbeheerd achter maar vergrendel het scherm of log uit.
- Na 30 minuten inactiviteit wordt het scherm vergrendeld.
- Er wordt automatisch gecontroleerd op het gebruik van goede wachtwoorden.

3.4 Wat doen bij vermoeden van misbruik?

Misbruik kan ontvreemding of onrechtmatig gebruik van een wachtwoord zijn.

- Verander het wachtwoord onmiddellijk
- Neem direct contact op met het aanspreekpunt informatieveiligheid, de dienst ICT en/of de systeembeheerder. Meldpunt datalekken: privacy@kov.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

- We voorzien zoveel mogelijk de “wachtwoord vergeten”-optie gebruiken. Afhankelijk van het platform of de voorafingestelde opties door gebruiken zullen hier 1 of meerdere herstelmogelijkheden beschikbaar zijn.
- Anders neem je persoonlijk contact op met de dienst ICT op https://help.kov.be. Zij zullen door middel van een wachtwoordreset een nieuw, éénmalig te gebruiken wachtwoord voorzien waarmee de gebruiker terug zal kunnen aanmelden.

3.6 Gebruik van wachtwoordmanagers of een wachtwoordkluis

Indien je te veel wachtwoorden moet onthouden, kan je gebruik maken van een wachtwoordkluis. Wachtwoord-kluizen 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. Meer info is terug te vinden in de brochure “Duiding rond het nieuwe wachtwoordbeleid”.

4 Gebruik van two-factor authenticatie

Indien je beheerderstoegang hebt op systemen 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 KOV vzw dan ook toegepast voor iedereen die toegang heeft tot systemen die vertrouwelijke info bevatten. Naast het beschermen van de info worden hiermee ook de systemen zelf beschermd. Voor de jongste leerlingen voorzien we in de toekomst toegangsbeperking gelimiteerd tot België. Voor oudere leerlingen raden we dezelfde 2 factorauthenticatie aan als de personeelsleden.

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 KOV vzw 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