**Beleid wachtwoorden**

**Doel**

Het doel van deze procedure is het omschrijven hoe op een correcte en veilige manier wordt omgegaan met wachtwoorden.

**Verantwoordelijkheden en bevoegdheden**

Alle gebruikers zijn verplicht sterke wachtwoorden te kiezen en op een verantwoorde en veilige manier met wachtwoorden om te gaan.

Alle gebruikers zijn verplicht incidenten met betrekking tot wachtwoorden te melden aan het aanspreekpunt informatieveiligheid.

Het aanspreekpunt informatieveiligheid neemt de nodige maatregelen om het incident op te lossen.

**Toepassingsgebied**

Deze procedure is van toepassing op alle personeelsleden van het CLB.

**Middelen**

Beheermodule wachtwoorden: bepaalde software die gebruikt wordt in het CLB voorziet de mogelijkheid om een beleid rond wachtwoorden te definiëren (soort en aantal karakters, duur geldigheid ...)

**Referenties**

Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming)

http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&rid=1

**Werkwijze**

**Kiezen van wachtwoord**

Kies voor alle toepassingen een complex en sterk wachtwoord. Kenmerken van een sterk wachtwoord:

* Het wachtwoord is hoofdlettergevoelig.
* Een wachtwoord moet minimaal 8 tekens lang zijn.
* Combineer cijfers, hoofdletters, kleine letters en symbolen. Een goed wachtwoord bevat minstens een van elk van deze elementen.
* Gebruik geen persoonlijke gegevens (bv. geboortedatum), bekende uitdrukkingen (bv. carpe diem), vaak voorkomende wachtwoorden (bv. 112233) of veel herhaling (bv. aaabbb111).
* Gebruik een lang wachtwoord.

Sterke wachtwoorden zijn doorgaans niet zo gemakkelijk om te onthouden. Je kan ook gebruikmaken van een wachtwoordzin die voor jou betekenis heeft. Als algemene regel geldt dat wachtwoordzinnen op grond van hun lengte veiliger zijn dan zogenaamd ‘sterke’ (complexe) wachtwoorden. Hoe kan je hiervoor te werk gaan? Neem een zin die je gemakkelijk kan onthouden. Neem van ieder woord de eerste letter en vervang bepaalde letters door leestekens, cijfers, hoofd- of kleine letters. Een voorbeeld: van ‘Ik eet graag biefstuk met frieten’ kan je een wachtwoord maken als ‘1kegBmF!’.

**Beschermen van wachtwoorden**

Wachtwoorden zijn strikt persoonlijk. Ze worden niet uitgewisseld met andere gebruikers. Geef je wachtwoord dus aan niemand door, zelfs als dit gevraagd wordt.

Een gebruiker mag anderen niet toelaten om met zijn wachtwoord en zijn toegangsrechten te werken.

Hergebruik geen wachtwoorden. Gebruik voor de diverse applicaties een totaal verschillend

wachtwoord. Vermijd het gebruik van hetzelfde wachtwoord voor werk en privé.

Het is een goede gewoonte om je wachtwoorden voor alle toepassingen geregeld te wijzigen (bv. om de drie maanden).

Belangrijk is ook hoe je met je wachtwoorden omgaat. Het is nutteloos om elke drie maanden je wachtwoorden te veranderen of een lange wachtzin te gebruiken om dan je wachtwoord in een document op je computer op te slaan of op een post-it op je computer te hangen. Wees dus voorzichtig met waar je je wachtwoorden bewaart en sla ze nooit zichtbaar of automatisch op bij het gebruik van een applicatie. Bewaar je wachtwoord niet in een browser, in je mail, in een Word-document, op een post-it bij je computer, in notitie op je smartphone.