VUB Informatieveiligheid en Privacy

How To – Wachtwoord beheer

Verantwoordelijke:
Chief Information Security Officer

Contact(en):
ciso@vub.be

Laatste update:
17 maart 2020

I. Overzicht

Een “How To …” document geeft informatie en/of hints en tips over een specifiek Informatieveiligheid en Privacy (IVP) onderwerp. Het bevat geen dwingende standaard/richtlijn, het geeft info over hoe een standaard/richtlijn kan toegepast worden.

Het is een ‘levend’ document en de kwaliteit is deels afhankelijk van de feedback van zijn lezers/gebruikers. De cover bladzijde geeft het contact e-mailadres waarnaar feedback kan gestuurd worden

Een “How To” document volgt geen formeel advies en goedkeuringsproces.

Dit How To document behandelt het beheer van wachtwoorden. Het werd voor publicatie geviseerd door de Directie ICT (DICT).

II. Wachtwoord beheer

Elke VUB-gebruiker is verantwoordelijk voor alle acties die onder zijn/haar VUB-gebruikersnaam uitgevoerd worden. Het is dus zeer belangrijk dat je VUB-wachtwoord onder alle omstandigheden beschermd wordt.

- ⇨ Een sterk wachtwoord is minimaal 12 karakters lang. Je kan gerust een zin gebruiken, inclusief spaties. Bv. “Ik en ik alleen ken mijn wachtwoord”.

  Indien de applicatie geen 12 karakters toe laat, gebruik dan het maximumaantal toegelaten karakters. Hier moet dan wel een combinatie van hoofd en kleine letters, cijfers en speciale tekens worden gebruikt (de ‘oude’ standaard).

  (Het huidige VUB-wachtwoord kan slechts 8 lang zijn. Aanpassing van het proces dat de VUB-wachtwoorden beheerd is in voorbereiding doch dit is tijdsintensief en er is momenteel geen implementatiedatum gekend.)

  Je kan je wachtwoordsterkte testen, b.v., op https://howsecureismypassword.net/. Test hier niet je wachtwoord dat je wil gebruiken, maar een gelijkaardig wachtwoord (gelijkaardig qua lengte en structuur).

- ⇨ Je moet je wachtwoord minimaal jaarlijks veranderen. Herbruik geen oude wachtwoorden of delen hiervan. Bv. verander “Het paard rijdt met de ruiter 2018” niet in “Het paard rijdt met de ruiter 2019”.

- ⇨ Verander je wachtwoord onmiddellijk na een incident of vermoeden van een incident. Bv.,
  - Na verlies van laptop of ander apparaat dat je gebruikt hebt om in te loggen;
  - Na een incident met een centraal systeem, VUB of extern, waarop je (ooit) hebt ingelogd;
  - Nadat je systeem door een virus werd besmet en hersteld werd.

- ⇨ Deel nooit je wachtwoord met anderen, ook niet met de VUB Service Desk of je leidinggevende. Indien iemand je wachtwoord vraagt moet je dit weigeren.

  Ben je afwezig en is het nodig dat een collega taken overneemt waarbij gebruik moet gemaakt worden van ICT-systemen waar deze geen toegang tot heeft, zorg er dan voor dat deze collega

waar nodig (tijdelijk) de benodigde toegang/gebruikersrechten heeft. 'Leen' je collega nooit je VUB-gebruikersnaam en wachtwoord!

Een nieuwe collega die nog geen gebruikersnaam/wachtwoord heeft even uit de nood helpen door je VUB-gebruikersnaam en wachtwoord met deze te delen is niet toegestaan. Vraag login gegevens voor nieuwe medewerkers tijdig aan.

Een bezoeker die even op WiFi wil doch geen gastaccount heeft mag ook geen gebruik maken van jouw VUB-gebruikersnaam en wachtwoord om op het VUB WiFi-netwerk in te loggen. Contacteer de helpdesk voor een gastaccount. Doe dit best voorafgaand aan het bezoek.

⇨ Gebruik je VUB-wachtwoord verbonden met je VUB-gebruikersnaam niet voor andere diensten (bv. Google mail, Facebook, …). Je VUB-wachtwoord dien je enkel met je VUB-gebruikersnaam te gebruiken.

⇨ Eén wachtwoord voor verschillende diensten (Gmail, Facebook, Online bankieren, …) gebruiken is een groot risico. Er moet maar één dienst gehackt worden, en de hacker heeft toegang tot al je diensten.

Gebruik je privé of professioneel meerdere diensten, dan is het onthouden van al deze verschillende wachtwoorden soms een onmogelijke taak. Overweeg dan het gebruik van een wachtwoord manager. Voorbeelden van gratis wachtwoord managers: LastPass, dashlane en KeePass. Doch ook hier best om je VUB-wachtwoord er niet in op te slaan.

⇨ Indien je privé of professioneel de "onthoud wachtwoord" functie van je webbrowser wil gebruiken (nooit gebruiken voor je VUB-wachtwoord!), activeer dan de optie om een algemeen wachtwoord op je browser te zetten. Je moet dan bij het opstarten van je browser slechts éénmaal dit algemeen wachtwoord in geven.

Hierdoor vermijd je dat andere gebruikers van je browser met behulp van deze functie op je diensten inloggen.

⇨ Schrijf je VUB-wachtwoord nergens op, sla het niet op in een bestand, vermeld het nooit in een e-mail.

⇨ Indien je een initieel/reset wachtwoord krijgt via e-mail, verander dit onmiddellijk.

⇨ Indien mogelijk gebruik Multi-Factor-Authenticatie (MFA). Hierbij moet je naast het invoeren van je gebruikersnaam en wachtwoord een tweede 'sleutel' ingeven om in te kunnen loggen. Voorbeelden van zo'n tweede sleutel zijn het ontvangen van een sms-code, het ontvangen van een aanmeldingsverzoek in een gekoppelde app op je smartphone of het overnemen van een app gegenereerde code. Alleen deze combinatie zorgt ervoor dat je toegang krijgt.

Door MFA te gebruiken ben je beter beschermt tegen misbruik van je wachtwoord.