



Frankelandgroep

Gouden regels informatiebeveiliging



Gebruik computerfaciliteiten alleen voor zakelijk gebruik



Maak geen gebruik van USB-sticks om persoonsgegevens op te slaan



Houd inloggegevens voor jezelf en leen je wachtwoord nooit uit aan collega's

- » Bewaar wachtwoorden op een veilige plek, dus niet in een agenda of op een post-it aan het beeldscherm.



Gebruik goede wachtwoorden

- » Voor anderen niet eenvoudig te raden en tegelijkertijd wel goed te onthouden. Het bestaat bij voorkeur uit een combinatie van letters, cijfers en één of meerdere speciale tekens.
- » Gebruik niet voor alles hetzelfde wachtwoord.



Laat je (actieve) werkplek niet onbeheerd achter (clear desk/clear screen)

- » Vergrendel je pc, of sluit deze af, wanneer je (tijdelijk) je werkplek verlaat, bijvoorbeeld voor een vergadering, lunch of afspraak. Dit doe je via Windows-L of via Ctrl-Alt-Del.
- » Laat geen vertrouwelijke gegevens, zoals dossiers of verslagen, onbeheerd achter op je bureau of in een niet afsluitbare kast.
- » Gooi vertrouwelijke gegevens nooit in een gewone prullenbak, maar maak hiervoor gebruik van vergrendelde papiercontainers of de papierversnipperaar.



Communiceer op een verantwoorde manier met en over cliënten/bewoners/collega's

- » Voer geen vertrouwelijke gesprekken op de gang waar iedereen kan meeluisteren.
- » Maak persoonsgegevens niet verder bekend dan noodzakelijk is voor het uitoefenen van je functie.
- » Wissel alleen gegevens uit als je zeker weet dat iemand een behandelrelatie heeft met de betreffende cliënt/bewoner.
- » Deel nooit meer informatie dan echt nodig is om je doel te bereiken.



Communiceer alleen op een veilige en verantwoorde manier

- » Gebruik alleen je zakelijke @frankelandgroep.nl e-mailadres om e-mail berichten te versturen.
- » Gebruik altijd het 'veilig verzenden' van Zorgmail voor communicatie van persoonsgegevens (ook naar de cliënt/vertegenwoordiger en externe organisaties).
- » Intern mailverkeer (tussen @frankelandgroep.nl adressen) wordt altijd automatisch beveiligd verzonden, zonder dat je daar iets voor hoeft te doen.
- » Gebruik geen sms, WhatsApp of vergelijkbare applicaties voor het verzenden van vertrouwelijke informatie cq. persoonsgegevens. Een veilig alternatief hiervoor is Siilo.
- » Controleer altijd de geadresseerde, zodat berichten niet per ongeluk bij een verkeerde ontvanger terecht komen.
- » Gebruik nooit gratis publieke diensten of apps, zoals Dropbox of OneDrive.
- » Zet geen mensen in de cc voor wie de informatie niet direct benodigd is.



Wees voorzichtig met verdachte e-mailberichten

- » Open geen e-mails van onbekende/verdachte afzenders. Klik niet op links of bijlagen uit dergelijke mails. Indien dit per ongeluk toch gebeurt, neem dan direct contact op met de afdeling ICT.



Kijk nooit uit nieuwsgierigheid in een dossier!



Herken en meld beveiligingsincidenten, via Topdesk

Voorbeelden van (mogelijke) incidenten zijn:

- » besmettingen met virussen en malware
- » een gestolen laptop
- » het versturen van een e-mail met gevoelige informatie naar het verkeerde e-mailadres.