# Gouden regels m.b.t. informatiebeveiliging en privacy

De  gouden regels voor het gebruik van informatie, informatiesystemen en netwerken.

Wij vragen om jouw aandacht!

Afhankelijk van jouw functie heb jij toegang tot diverse informatiesystemen binnen Curio. Wij willen je erop attenderen dat het gebruik van deze systemen verbonden is aan een aantal verplichtingen. Met deze ***gouden regels*** vatten wij de belangrijkste hiervan samen. Wij verzoeken je deze goed door te lezen omdat zij deel uitmaken van het verantwoord omgaan met (persoons)gegevens.

- **Wachtwoorden zijn strikt persoonlijk**
  Je wachtwoorden zijn strikt persoonlijk en dienen uitsluitend door jou gebruikt te worden om toegang te krijgen tot de betreffende systemen. Geef je wachtwoord dus niet aan derden, of aan een collega of je manager, en bewaar ze op een *veilige* plek, dus *niet* in je agenda of op een geel briefje! Als iemand met kwade bedoelingen namelijk jouw wachtwoord weet en hier misbruik van maakt, ben jij verantwoordelijk.

  Tip: Gebruik een wachtwoordmanager om je wachtwoorden veilig te bewaren. Een voorbeeld van zo'n wachtwoordmanager is bijvoorbeeld LastPass.

- **Clear desk / clear screen policy**
  De vertrouwelijke omgang met (persoons)gegevens houdt o.a. in dat elke werkplek zodanig is ingericht, dat onbevoegden in jou afwezigheid niet aan deze gegevens kunnen komen.
  Dat betekent dat jij je computer bewust dient te vergrendelen wanneer jij je werkplek verlaat en dat je geen vertrouwelijke gegevens, zoals dossiers of verslagen, onbeheerd op je bureau of in een niet afsluitbare kast achterlaat.

  Tip: je kunt je computer Makkelijk vergrendelen door de volgende toets combinatie te gebruiken ⊞ + L

- **Beveilig mobiele apparatuur met een wachtwoord of pincode**
  Als je je e-mail van het werk op je mobiele telefoon of ander draagbaar apparaat hebt geïnstalleerd, zorg er dan voor dat je mobiele telefoon met een wachtwoord of pincode is beveiligd. Zo is er bij verlies of diefstal niet meteen gevaar dat onbevoegde personen bij vertrouwelijke informatie kunnen komen.

  Tip: je kunt je e-mail bij verlies van je telefoon via de Outlook Web app op de portal van Curio op afstand wissen. Op deze manier kunnen de mails niet meer door onbevoegden worden gelezen. Voor hulp bij deze actie kun je altijd contact opnemen met de Servicedesk van Curio (8080).

- **Open alleen e-mails die je vertrouwt**
  De meesten van ons krijgen dagelijks e-mails. Of het nu gaat om ongevraagde spamberichten of berichten van vrienden of collega's, ze zouden allemaal een virus, worm of Trojan horse bij zich kunnen hebben, waarmee je computer helemaal overhoop kan worden gehaald. En zelfs wanneer zij geen bijlage hebben, kunnen ze de aandacht trekken met een koppeling die de lezer naar een geïnfecteerde website leidt in een poging je computer in gevaar te brengen.

  Tip: Als je twijfels hebt over een e-mail — je kent de afzender niet of het onderwerp of de bijlage roept vraagtekens op — open die e-mail dan niet! Verwijder in dit geval het bericht inclusief de bijlage.

- **Controleer het adres van de websites die je bezoekt**

Als je een website bezoekt waar je gevoelige gegevens (bijvoorbeeld persoonsgegevens) in moet voeren, kijk dan of de URL begint met https (let op de s) en of er een hangslotje te zien is in de adresbalk. Beiden geven aan dat je op een beveiligde website bent.

Tip: zie je geen hangslotje of https? Verstrek dan geen gevoelige gegevens via deze website.

- **Ga zorgvuldig om met USB-sticks**
  USB-sticks worden steeds vaker gebruikt om virussen te verspreiden en gegevens te vernietigen of te stelen. Gebruik daarom je USB-stick niet zomaar op elke computer en sluit geen vreemde USB-sticks aan op jouw computer. Beveilig daarnaast je USB-stick als je een USB-stick gebruikt om werkdocumenten mee naar huis te nemen. Zo is er minder kans dat bij verlies van de USB-stick de gegevens door derden gelezen kunnen worden (in geval van persoonsgegevens noemen we dit een datalek).

  Tip: Beveilig je USB-stick door bijvoorbeeld Bitlocker te gebruiken (dit werkt vanaf Windows 7).

**Handige website met veel informatie:**

**https://veiliginternetten.nl/**