

Gouden regels Veilig thuiswerken – via VMware

COVID-19



 Hilversum
Mediastad



Let *extra* goed op bij
het verwerken van
persoonsgegevens

Wanneer je thuiswerkt vragen we je om het onderstaande te doen

- Maak gebruik van een **vertrouwd** en **beveiligd** (wifi)netwerk.
- Maak gebruik van **VMware** om op een veilige manier te werken.
- Houd rekening met een langere reactiesnelheid door gelimiteerde netwerkcapaciteit, je ziet dan bijvoorbeeld dat je muis trager werkt.
- Gebruik Webmail liever niet.
- Ga bewust om met informatie thuis en let erop wat je bespreekt in berichtenapps of tijdens een videoconference.

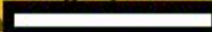
Extra alert zijn op cybercrime

- Houd rekening met het ontvangen van phishingmails en valse e-mails omtrent het Coronavirus. Het is bekend dat criminelen gebruik maken van de huidige ontwikkelingen door het versturen van phishingmails of het verspreiden van malware. Ga niet in op de phishingmail.
- Klik niet op links in e-mailberichten, open geen onbekende bijlagen en vul geen gegevens in bij e-mailberichten die u niet verwacht of van een onbekende afzender zijn.
- Download geen programma's die over het Corona virus gaan. Er is bijvoorbeeld een malafide app 'COVID19 Tracker' in omloop deze installeert de CovidLock ransomware op apparaten met het Android besturingssysteem. We kunnen verwachten dat er nog meer van dit soort cybercrime rond zal gaan, wees alert.

Ook als je thuiswerkt ga je integer om met informatie

- Je bent verplicht tot geheimhouding van alle vertrouwelijke informatie.
- Sla geen bedrijfsinformatie (langdurig) op op je privé apparatuur, nu je via VMware kunt werken vragen we je om de informatie naar de Hilversum omgeving te verplaatsten.
- De gegevens (data) die je voor je werk gebruikt hebben bescherming nodig; denk aan gebruik van sterke wachtwoorden en schermbeveiliging.
- Lock thuis ook je scherm als je even iets anders gaat doen.
- Met persoonsgegevens of vertrouwelijke onderwerpen ga je uiterst discreet om.

Ook als je thuiswerkt moet je erop letten dat je veilig met de gegevens van burgers, instellingen en bedrijven in Hilversum blijft omgaan

- Als je een malafide e-mail hebt ontvangen, meldt dit dan bij ons ICT team via 
- Als je twijfelt dan kun je van de privacy of security officer hulp krijgen bij een datalek of informatiebeveiligingsincident. Mail naar 
- Je meldt datalekken en informatiebeveiligingsincidenten zo snel mogelijk. Er is een meldingsformulier op [intranet](#).