



De Regio blijft doorwerken tijdens de coronacrisis. Wie dat kan, doet dat thuis. Maar let op: voor cybercriminelen is deze crisis een kans om gevoelige data buit te maken. En een foutje is snel gemaakt, waardoor gevoelige gegevens op straat kunnen komen te liggen. Volg onderstaande richtlijnen en voorkom dat er gegevens over inwoners of collega's in verkeerde handen vallen.

Door het naleven van deze regels kunnen we zo zorgvuldig en zo veilig mogelijk thuis werken met middelen die door de Regio beschikbaar zijn gesteld (smartphone, laptop) of met eigen apparatuur.



1. Werk bij voorkeur met de middelen die door de Regio beschikbaar zijn gesteld, zoals iPhone, iPad en laptop;
2. Indien eigen apparatuur wordt gebruikt (computer, laptop, privételefoon), dan mag op de schijven hiervan geen bedrijfsinformatie en gevoelige (persoons)informatie worden opgeslagen;
3. Werk voor wat betreft vak-applicaties zoveel mogelijk binnen de beveiligde werkomgeving via Ericom Blaze. Kun je in je werk volstaan met enkel de mail dan is het dringend verzoek om dat zoveel mogelijk via webmail te doen;
4. Gebruik altijd je werkmailadres en werktelefoonnummer (indien beschikbaar) voor zakelijke communicatie;
5. Wees voorzichtig met het gebruik van (video)chatdiensten. Bellen en SMS is nog steeds het makkelijkst en veiligst. Over de mogelijkheden om online te vergaderen (waaronder videobellen) is al eerder een [stappenplan](#) gecommuniceerd waarin eerst naar de veiligste opties moet worden gekeken en pas in laatste instantie naar de minst veilige opties.
6. Bewaar het gebruikerswachtwoord om in je je laptop te komen niet op een briefje op of in de laptop maar leer het uit je hoofd;
7. Sla geen documenten lokaal op je laptop op, zeker niet als je huisgenoten van dezelfde laptop gebruik maken. Andersom: bescherm jezelf en je huisgenoten tegen het uitlekken van persoonlijke documenten als de laptop weer terug moet naar ICT.
8. Ga zorgvuldig om met mobiele apparatuur: niet onbeheerd achterlaten in bijvoorbeeld een vervoermiddel of een ruimte waarin andere personen aanwezig zijn;
9. Indien de werkplek wordt verlaten en er andere mensen in de woning aanwezig zijn, dien je Ericom Blaze (tijdelijk) af te sluiten;
10. Gegevens die je verwerkt namens de Regio zijn vertrouwelijk, dus niemand kijkt mee/luistert mee. Wees net als altijd extra voorzichtig met bijzondere persoonsgegevens, zoals medische gegevens;
11. Laat eventueel in bezit zijnde fysieke documenten van de Regio niet onbeheerd en berg ze goed op. Wil je ze vernietigen, neem ze dan t.z.t. weer mee naar de Regio en gooi ze in de daarvoor bestemde zilveren papiercontainers;
12. Neem geen fysieke documenten/dossiers met persoonsgegevens mee naar huis, tenzij het praktisch echt niet uitvoerbaar is om dit op een andere manier te doen, bijvoorbeeld door te digitaliseren/scannen. Desnoods maak je gebruik van een versleutelde USB-stick (te verkrijgen bij de ICT servicedesk);
13. Let op phishingmails/sms-jes. Dit zijn berichten die door kwaadwillenden aan mensen worden gestuurd om hen aan de hand van een actueel thema (zoals nu corona) te verleiden persoonlijke gegevens te verstrekken. Krijg je berichten die je niet verwacht of die van een onbekende afzender zijn? Klik dan niet op links in deze berichten, open geen bijlagen en vul geen gegevens in. Zie hierover ook [dit](#) eerdere bericht op de Binnenband;
14. Wees voorzichtig met het gebruik van cloud- of opslagdiensten, zeker wanneer deze gratis zijn. Want het zou kunnen dat zo'n dienst juist gratis is omdat de aanbieder je gegevens gebruikt voor andere doeleinden of omdat geen aandacht is besteed aan beveiliging.
15. Zorg dat je altijd goed bereikbaar bent voor je collega's (en externen/derden) voor vragen en overleg.
16. Probeer te voorkomen dat een datalek ontstaat met deze [tips](#).
17. Neem je verantwoordelijkheid voor informatiebeveiliging als er toch iets fout gaat of als je verdachte zaken ziet en meld dit direct bij de ICT Service Desk (via (035) 692 62 00 of meldpuntdatalek@regiogv.nl) of maak een [melding](#) via de Binnenband.