COA Centraal Orgaan opvang asielzoekers

6 belangrijke regels voor veilig digitaal werken

Met de nieuwe COA ICT-middelen kun je meer flexibel en mobiel werken. Deze flexibiliteit brengt verantwoordelijkheden met zich mee. Iedereen moet zorgvuldig omgaan met (vertrouwelijke) informatie en persoonsgegevens die op deze middelen staan. Om je hierbij te helpen zijn deze 6 belangrijke regels voor veilig digitaal werken opgesteld.

1 Voorkom misbruik en diefstal

- Hanteer de clean desk & clear screen principes: berg vertrouwelijke informatie op en vergrendel bij afwezigheid je scherm.
- Laat laptop of 2-in-1 laptop, tablet en smartphone nooit onbeheerd achter.
- Houd inloggegevens voor jezelf en schrijf ze niet op.
- Beveilig je smartphone en tablet met je vingerafdruk en/of een pincode.

2 Ga binnen en buiten de COA-locaties zorgvuldig om met vertrouwelijke informatie

- Zorg ervoor dat niemand kan meekijken of -luisteren als je met vertrouwelijke informatie werkt. Wees je bewust van jouw omgeving en die van je gesprekspartner bij een telefoongesprek, Skype of e-mail.
- Laat vertrouwelijke informatie niet onbeheerd achter.
- Stuur geen persoonsgegevens via e-mail naar partijen buiten het Rijk.
- Wissel alleen informatie uit via de systemen van het COA (Blackberry Work en Citrix). Deze zijn goed beveiligd tegen inbreuk. Daardoor kun je ook veilig gegevens uitwisselen via WiFi of 4G op andere locatie.

3 Ga veilig om met zakelijke informatie op privé apparaten

Het is niet de bedoeling dat je privé-apparaten zakelijk gebruikt, maar soms is het noodzaak. Neem dan onderstaande regels in acht:

- Zorg voor een gedegen en up-to-date virusscanner en fire-wall, ingesteld op het hoogste veiligheidsniveau.
- Plaats nooit zakelijke informatie op privé-apparaten. Laat die informatie binnen de centrale beveiligde ICT-omgeving van het COA (Blackberry Work en Citrix).
- Sla geen zakelijke of vertrouwelijke informatie op in de cloud (Google Drive, Dropbox, Evernote, etc.).
- Stuur geen zakelijke e-mail naar je privéaccount.

4 Ga voorzichtig om met verdachte telefoontjes, e-mails en websites

- Geef nooit inloggegevens aan anderen. Ook niet als je daar om gevraagd wordt via de telefoon, e-mail of op een website.
- Open nooit verdachte bestanden, klik nooit op verdachte links, pop-ups en banners.
- Vertrouw je het niet: hang op, klik weg en neem contact op met de ICT Servicedesk (088 - 715 73 74).

5 Wees zorgvuldig in online communicatie en social media

- Wees je bewust van wat je deelt op social media. Ook als privépersoon ben je ambassadeur van het COA.
- Communiceer niet over zaken die schadelijk kunnen zijn voor het COA.
- Gebruik WhatsApp en sms alleen voor informele communicatie. Deel geen vertrouwelijke informatie via deze kanalen.
- Wees altijd zorgvuldig, betrouwbaar, positief en respectvol.
- Meer weten? Check de COA-Gedragsrichtlijnen Sociale Media.

6 Spam, phishing mail of datalek? Meld het!

Krijg je te maken met spam, phising, malware of virussen, of vermoed je dat vertrouwelijke informatie of persoons-gegevens zijn ingezien door onbevoegden, meld dit dan direct bij de ICT Servicedesk (088 715 73 74).

Bij twijfel of vragen:

neem contact op met de ICT Servicedesk (088 - 715 73 74)