



Gouden regels voor privacy en security

De gouden regels voor privacy en security vormen de basis voor het veilig gebruik van informatie, informatiesystemen en netwerken. Het CBR beschikt over veel vertrouwelijke informatie. Het is van belang dat je als gebruiker zorgvuldig en op een integere wijze met deze informatie omgaat. Afhankelijk van je functie heb je toegang tot diverse informatie en systemen van het CBR. Wanneer je deze wilt gebruiken moet je je houden aan regels om de vertrouwelijkheid van de informatie te kunnen garanderen. De belangrijkste regels vind je in dit document. Lees deze regels goed door en pas ze toe in je dagelijks werk.

1. Fysieke toegang

- Voorkom ongeautoriseerde toegang tot onze gebouwen en systemen.
- Je toegangspas is strikt persoonlijk: leen hem niet uit en meld vermissing direct bij facilitaire zaken via 088 227 55 55.
- Draag je toegangspas altijd zichtbaar.
- Voorkom het 'meelopen' via jouw persoonlijke toegangspas.
- Haal bezoekers op bij de receptie en begeleid ze weer naar de uitgang.
- Spreek mensen zonder toegangspas of bezoekerspas aan en vraag wie zij zoeken.

2. Digitale toegang

- Gebruik altijd een eigen persoonlijk wachtwoord of pincode voor je mobiele apparatuur.
- Houd wachtwoorden en pincodes voor iedereen geheim. Geef deze ook nooit aan een collega.
- Gebruik niet overal hetzelfde wachtwoord of dezelfde pincode.

3. Internet, intranet en e-mail

- Internet en e-mail zijn voor zakelijk gebruik; incidenteel persoonlijk gebruik is toegestaan.
- Wees alert op virussen en spyware en open geen berichten en bijlagen, als er twijfels zijn over bijvoorbeeld de verzender.
- Denk eraan dat mobiele apparatuur ook virusgevoelig is.
- Bezoek geen discriminerende, aanstootgevende of illegale sites.
- Weet met wie je communiceert en controleer de adressering van je e-mails.
- Ga zorgvuldig om met internet en e-mail.
- Verstuur vertrouwelijke informatie per e-mail versleuteld.

4. Thuiswerken

- Zet geen vertrouwelijke informatie op privé apparatuur.
- Vervoer vertrouwelijke informatie op draagbare apparatuur alleen versleuteld.

5. Geheimhoudingsplicht

- Deel informatie over klanten, opleiders, medewerkers en andere informatie waarvan je kunt aannemen dat die vertrouwelijk is, nooit met derden.
- Wees voorzichtig met wat je aan derden vertelt over de inhoud van je werk.
- Voorkom meekijken en meeluisteren.
- Houd werk en privé gescheiden: zet geen informatie over je werk op sociale media.
- Controleer de identiteit van de betrokkene goed voordat je (telefonisch) informatie verstrekt.
- Gebruik en verstrek geen vertrouwelijke informatie als dat niet noodzakelijk is voor het verrichten van je werkzaamheden. Deel en raadpleeg geen vertrouwelijke informatie vanuit sensatie of pure nieuwsgierigheid.
- Gebruik vertrouwelijke informatie alleen voor de daarvoor vastgestelde doelen.

6. 'Clean desk' en 'clear screen'

- Zorg dat vertrouwelijke informatie - op papier of elektronisch - niet zomaar kan worden gelezen, gekopieerd of meegenomen (clean desk).
- Vergrendel je pc/laptop bij het verlaten van je werkplek met de toetscombinatie 'Windows toets + L' (clear screen).
- Gooi interne of vertrouwelijke informatie niet zomaar weg, maar gebruik de speciale papiercontainers en/of vernietig de informatie(drager).

7. Voorkom verlies en diefstal

- Voorkom verlies en diefstal; berg je laptop veilig op.

8. Bewustzijn

- Wees bewust, zorgvuldig en alert en houd elkaar scherp op de naleving van deze regels.

9. Normen en waarden van het CBR

- Houd je aan de gedragscode internet, intranet en e-mail.
- Houd je aan de gedragscode integriteit.
- Houd je aan de regeling grensoverschrijdend gedrag.
- Houd je aan de regeling zorgvuldig gebruik van informatie.

10. Meldingen

- Meld datalekken en informatiebeveiligingsincidenten via melden.datalekken@cbr.nl.
- Meld fraude via melding@cbr.nl.
- Meld een verloren toegangspas via telefoonnummer 088 227 55 55.
- Meld overige incidenten bij de ICT Servicedesk, bel 5800 of mail ICT.servicedesk@cbr.nl.
- Kijk op intranet: Organisatie > Security & privacy.