

Gouden regels informatiebeveiliging & privacy – externen

Publicatiedatum: 09-05-2025

Documentbeheerders: Security officer compliance

Proceseigenaar: Manager IKP

Bij Bevolkingsonderzoek Nederland hanteren we een aantal gouden regels voor informatiebeveiliging en privacy om onze werkomgeving veilig te houden. Je bent verplicht je aan deze gouden regels te houden.

1. **Clear screen!** Lock je scherm, ook wanneer je slechts 5 seconden van je werkplek bent!
(Windows toets + L)
- **Clean desk!** Ruim je bureau op. Wanneer je je werkplek verlaat voor een overleg of aan het einde van de werkdag laat dan geen spullen achter op je bureau. Papier met vertrouwelijke informatie dat je niet meer nodig hebt, in de papierversnipperaar of in de container voor vertrouwelijke stukken. Laat je sleutel/tag voor toegang tot het pand en tokens (YubiKey) voor toegang tot systemen niet onbeheerd achter. De YubiKey kun je opbergen in een sleutelkast op de kijklocatie of je beheert deze persoonlijk. Meld verlies direct via Topdesk.
2. Wees je bewust van **de vertrouwelijkheid van bepaalde documentatie**, dit is bij een groot aantal documenten onderaan de pagina terug te vinden, en dat documenten die bedoeld zijn voor intern gebruik bijvoorbeeld niet naar je privé emailadres worden gestuurd.
3. Houd je **wachtwoord geheim**. Gebruik bij voorkeur een wachtwoordkluis/-manager. Gebruik Keeper als wachtwoord kluis deze kan je aanvragen via Topdesk.
4. **Need-to-know / Need-to-use:** moet je echt bij deze gegevens kunnen? Niet nodig is niet kijken! Maak eventueel een melding in Topdesk als je onterecht iets mag inzien.
5. **Voorkom** tijdens je werk **meekijken en meeluisteren** door derden. Je kunt via Topdesk een aanvraag doen voor een privacy screen voor je laptop.
6. Denk goed na welke informatie je deelt, met name die te herleiden is tot een persoon. **Veilig mailen via Zivver** is verplicht bij noodzakelijk delen van (privacygevoelige) informatie met derden. Echter wanneer je gebruik maakt van Outlook op je mobiele telefoon of webmail, mag je geen vertrouwelijke gegevens versturen.
7. Vermijdt zoveel mogelijk **openbare wifi-netwerken of publieke hotspots (trein, cafés, winkels)**, maak dan bij voorkeur gebruik van de mobiele hotspot van je zakelijke telefoon om via je werklaptop te verbinden met het internet.
8. **Meld incidenten** zoals virussen, diefstal en verlies direct in TOPdesk en bij datalekken ook telefonisch bij team IB&P!
9. **Gebruik geen externe opslag** zoals o.a. USB-stick USB-disk tenzij deze versleuteld is , of opslag in de Cloud anders dan Teams of OneDrive van de organisatie