De 10 gouden regels iBewustzijn

Binnen

1. Laat geen onbevoegden toe in onze gebouwen en op onze werkplekken

- Begeleid bezoekers zoveel mogelijk in het pand. Zo voorkom je dat ze verdwalen en is voor je collega's duidelijk voor wie de bezoeker komt. Draag je rijkspas bij voorkeur zichtbaar en motiveer anderen dat ook te doen.
- Spreek onbekende personen op jouw afdeling aan en vraag of je ze naar een collega of vergaderzaal kunt begeleiden
- Leen nooit je persoonlijke toegangspas uit aan collega's of anderen. Dat is niet toegestaan.

2. Voorkom misbruik en diefstal

- Doe aan *clear desk & clear screen*: berg vertrouwelijke informatie op achter slot en grendel en vergrendel je digitale werkplek als je even weg bent.
- Laat digitale gegevensdragers (laptop, smartphone, usb-stick) nooit onbeheerd achter.
- Gooi gebruikte gegevensdragers, zoals cd-roms of apparaten met een harde schijf niet zomaar weg. Lever ze in op het serviceplein zodat ze op een veilige manier kunnen worden vernietigd.
- Houd wachtwoorden voor jezelf en schrijf ze niet op.
- Vermoed je toch dat er gegevensdragers gestolen zijn? Meld dit bij de Centrale meldkamer (tel.nr. 070 - 751 6060). Vermoed je dat er vertrouwelijke informatie door onbevoegden is ingezien, meld dit dan bij je leidinggevende en – als het gaat om staatsgeheimen of departementaal vertrouwelijke informatie – de Beveiligingsautoriteit (BVA).

3. Ga vertrouwelijk om met informatie

- Zorg dat gevoelige informatie, fysiek of digitaal, in een veilige of afgeschermde omgeving blijft en 'lek' dus geen informatie in persoonlijke- en e-mailcommunicatie.
- Stuur e-mails niet automatisch door naar een mailadres buiten de rijksoverheid.

4. Zie je een incident? Meld het dan

- Technische incidenten (bijvoorbeeld een virus): meld dit bij de ICT-servicedesk: servicedesk van SSC-ICT, tel.nr. 070 - 426 7447.
- Meld overige beveiligingsincidenten (bijvoorbeeld diefstal of verlies) aan de Centrale meldkamer (tel.nr. 070 - 751 6060). Schakel direct bureau Beveiligingsambtenaar (BVA) in als er mogelijk vertrouwelijke informatie in handen is gekomen van onbevoegden en meld dit ook aan je leidinggevende.
- Bij integriteitskwesties kun je ook terecht bij de Vertrouwenspersonen binnen BZK. Je vindt hun contactgegevens op Rijksportaal.

Buiten

5. Zorg voor optimale beveiliging van mobiele apparaten met zakelijke informatie

- Gebruik een privé apparaat alleen voor zakelijke informatie als deze voorzien is van een Good-omgeving door de ICT-servicedesk van BZK.
- Sla zakelijke informatie op je smartphone of tablet alleen op in de Good-omgeving, strikt gescheiden van privé-informatie.
- Probeer bij het installeren van apps na te gaan of ze geen beveiligingsrisico vormen. Apps met veel en hoge waarderingen zijn doorgaans betrouwbaarder. Ga ook na welke toegangsrechten de app vraagt op je device: als je een reisplanner installeert is het bijvoorbeeld niet logisch dat deze toegang vraagt tot je adresboek.
- Op je werkplek (laptop of desktop) mag je zelf geen software installeren.
- Bij reparatie of verkoop van een privé apparaat dat je zakelijk hebt gebruikt: wis alle informatie door het toestel terug te zetten naar de fabrieksinstellingen en verwijder je geheugenkaart.

Achter je scherm

6. Neem zakelijke informatie alleen goed beveiligd mee buiten kantoormuren

- Zorg ervoor dat er geen onbevoegden mee kunnen kijken of luisteren als je met zakelijke informatie werkt, bijvoorbeeld in de trein of andere openbare ruimten.
- Houd zakelijke informatie altijd bij je.
- Verander direct je wachtwoorden als je vermoedt dat deze zijn gezien door anderen.
- Gebruik het liefst alleen zakelijke digitale gegevensdragers geleverd door SSC-ICT Haaglanden waarop de informatie wordt versleuteld, zoals beveiligde USB-sticks. Voor vertrouwelijke informatie is het gebruik van deze gegevensdragers zelfs verplicht.

7. Ga voorzichtig om met verdachte websites en informatieverzoeken

- Geef nooit inloggegevens zoals wachtwoorden af. Verstrek geen persoonsgebonden informatie, zoals creditcardgegevens of je personeelsnummer, als je niet zeker bent van de identiteit van de vrager of website.
- Open alleen links in en bijlagen bij e-mails als je de afzender vertrouwt en het mailadres herkent. Ontvang je een e-mail die je niet vertrouwt? Gooi deze niet direct weg, maar bel eerst de ICT Servicedesk om er melding van te maken.
- Controleer of het webadres in de adresbalk van je browser afwijkt van wat je verwacht voordat je inlogt of bestanden download. Ga na of een inlogpagina of een pagina met invulvelden wel voorzien is van een beveiligde (https) verbinding.
- Klik nooit op links, pop-ups en banners als je twijfelt of je ze kunt vertrouwen. Door met de muisaanwijzer op een link te staan, zonder te klikken, kun je linksonder in je browserscherm vaak het webadres zien waar je naartoe geleid wordt. Controleer of de site een adres heeft dat je kent of kunt verwachten.

8. Zorg dat je computer goed beveiligd is en voorzien is van actuele software

- Zorg, zeker als je je thuis-pc of laptop ook voor je werk gebruikt, altijd voorzien is van actuele antivirus-software en stel in dat je overige programma's zichzelf automatisch bijwerken.

In the cloud

9. Wees je bewust van de risico's van clouddiensten

- Gebruik diensten in de 'cloud', zoals Google Docs, Dropbox, Whatsapp, Pleio en Yammer nooit om vertrouwelijke informatie op te slaan of uit te wisselen.
- Maak alleen gebruik van clouddiensten op het moment dat je zeker bent van de impact en risico's. Zorg dat je weet hoe en waar de diensten je gegevens opslaan en wat ze er volgens hun algemene voorwaarden mee mogen doen.
- Besef dat gedeelde informatie in de cloud niet zomaar ter beschikking blijft voor het departement en daarom ook binnen het departement moet worden bewaard.

10. Houd je aan de Rijksvoorschriften voor online communicatie

- Houd er bij privégebruik van sociale media rekening mee dat je een ambassadeur bent van je organisatie. Scherm je profielen goed af voor derden als je strikt als privé persoon online actief bent.
- Communiceer niet over zaken die schadelijk kunnen zijn voor het ministerie of de ministers.
- Wees altijd zorgvuldig, betrouwbaar en respectvol.
- Neem kennis van de Uitgangspunten Online Communicatie Ambtenaren die je vindt op Rijksportaal.