

In het gebouw

- Bezoekers altijd begeleiden
- Onbekenden zonder (bezoekers)pas of begeleiding aanspreken: Stel je voor en vraag of je kunt helpen. Begeleid de gast.

Vermoed je dat vertrouwelijke informatie in handen is gevallen van onbevoegden?

Meld dit direct bij je afdelingshoofd!

Op je werkplek

- Wie kan je scherm zien als je er vertrouwelijke informatie op toont?
- Wie kan je horen tijdens vertrouwelijke gesprekken ?

Digitaal slot

- Versleutel informatie op digitale gegevensdragers
- Vergrendel altijd je scherm, ook al moet je maar even naar het toilet. Ctr+alt+del en enter of windowstoets-L indrukken kost maar een paar seconden.
- Hou wachtwoorden geheim; Deel je wachtwoord met niemand en zorg voor een sterk wachtwoord

Cleardesk

- Laat geen digitale gegevensdragers op je bureau liggen of in je computer zitten.
- Berg vertrouwelijke informatie op papier of digitale gegevensdragers op achter slot en grendel.
- Versnipper vertrouwelijke informatie op papier als je het niet meer nodig hebt of gooi het in de speciale containers.

Achter het scherm

- Verdachte e-mails **niet openen**
- Als een betrouwbaar uitziende e-mail een **verdachte boodschap** bevat, **bespreek** deze dan met collega's, ook bijvoorbeeld een e-mail die waarschuwt voor een eerdere phishingmail
- Reageer niet op deze mails
- Ga voorzichtig om met verdachte internetsites.
- Open nooit verdachte bestanden
- Klik nooit op verdachte links, pop-ups en banners
- Check of privacygevoelige, vertrouwelijke informatie verstrekt mag worden
- Verzend gegevens op een veilige wijze (SFTP)
- Stuur geen bedrijfsgegevens of privacygevoelige gegevens naar je privé mailadres
- Gebruik geen persoonlijke BsGW emailaccount voor communicatie met belastingplichtigen of derden. Maak gebruik van het CRM-systeem.

VOORBEELDEN VAN MOGELIJKE OORZAKEN VOOR EEN DATALEK

- EEN KWIJTGERAAKTE USB-STICK
- EEN GESTOLEN LAPTOP
- EEN INBRAAK DOOR EEN HACKER
- VERZENDING VAN E-MAIL WAARIN DE E-MAILADRESSEN VAN ALLE GEADRESSEERDEN ZICHTBAAR ZIJN VOOR ALLE ANDERE GEADRESSEERDEN
- EEN CALAMITEIT ZOALS EEN BRAND IN EEN DATACENTRUM
- GEBROKEN ENCRYPTIE/BEVEILIGING WAARDOOR TOEGANG TOT PERSOONSgegevens VOOR ONBEVOEGDEN ONTSTOND (BIJV. GELEKT WACHTWOORD VAN PIMS/CLOUD/TEAMSITE, ETC.)
- VERLOREN EN Vernietigde PAPIEREN MET PERSOONSgegevens OF BEDRIJFSgegevens (VERLIES VAN INFORMATIE)
- ONGEAUTORISEERDE TOEGANG VAN EEN LAPTOP, TABLET OF SMARTPHONE MET BEDRIJFSgegevens/PERSOONSgegevens

Werk veilig!!!

Informatiebeveiliging



informatie

- Er is een verschil tussen uitlatingen als privépersoon en als ambtenaar in functie.
- Publiceer nooit vertrouwelijke informatie op openbare netwerken of in de openbare cloud.

Thuiswerken

- Zorg dat je computer thuis voorzien is van een actuele virusscanner
- Maak enkel gebruik van de netwerkomgeving van BsGW met token om thuis te werken. Werk niet lokaal op je PC.
- Kopieer geen bestanden van je lokale computer naar de netwerkomgeving van BsGW.

Onderweg

- Meld verlies of diefstal van een mobiel apparaat direct aan het afdelingshoofd deze zal de helpdesk informeren zodat de data op afstand kunnen worden gewist.

Vermoed je dat je slachtoffer bent
geworden van phishing?
Heb je een verdachte mail ontvangen?
Vermoed je een virus?

Meld dit direct bij je afdelingshoofd!

- Activeer de app find my iphone en stuur laatste locatie op je mobiel BsGW-apparaat
- Versleutel de gegevens op een USB-stick

Sociale media

- De ambtenaar is een ambassadeur van zijn organisatie en integriteit is essentieel en vanzelfsprekend.
- Communiceer niet over zaken die schadelijk kunnen zijn voor je werkgever of collega's.
- De verantwoordelijkheid en de rol van ambtenaren zijn online en offline gelijk.

VOORBEELDEN VAN PERSOONSgegevens

- NAAM		
- ADRES		
- WOONPLAATS		
- POSTCODE		
- IP-ADRES		
- BANKREKENINGNUMMER		
- FOTO		
- MEDISCHE GEGEVENS		
- KADASTRALE INFORMATIE		
- BSN-NUMMER		
- TELEFOONNUMMER		
- KENTEKEN		
- GEBOORTEDATUM		

Werk veilig!!!