



8 Vuistregels voor informatiebeveiliging

it starts here.



1 Ga zorgvuldig om met informatie

- Houd de werkplek (of vergaderruimte) netjes.
- Berg informatiedragers op in een lade of kast die je kunt vergrendelen of verwijder ze op de juiste manier (versnipperaar, vergrendelde prullenbak).
- Schakel alle apparatuur volledig uit voordat je het kantoor verlaat om te voorkomen dat informatie verloren gaat.
- Neem altijd je persoonlijke spullen mee.
- Deel vertrouwelijke zakelijke informatie of bestanden alleen via beveiligde kanalen.
- Wees je ervan bewust met wie je informatie deelt.
- Controleer de inhoud en ontvanger(s) van de e-mails voordat je ze verstuurt.
- Voorkom dat anderen vertrouwelijke informatie op jouw scherm zien.

2 Ga veilig om met je wachtwoorden en computer

- Houd je mobiele apparatuur bij je.
- Laat je apparatuur nooit onbeheerd achter.
- Vergrendel je computer wanneer je jouw werkplek verlaat.
- Gebruik hoezen, cases of skins om jouw apparatuur te beschermen.
- Jouw toegangspas, wachtwoorden, pincodes en sleutels zijn alleen voor jou bedoeld; deel deze niet met anderen.
- Beveilig je apparatuur met een wachtwoord, pincode of biometrische gegevens en gebruik waar mogelijk multifactor-authenticatie.
- Zorg ervoor dat je computer en applicaties zo snel mogelijk worden bijgewerkt.
- Beveilig je e-mail met 2FA / MFA. Verzoeken tot het resetten van jouw wachtwoord van veel services komen in je e-mail terecht. Toegang tot je e-mail betekent toegang tot veel services.

3 Wees omgevingsbewust

- Communicatie (en het delen van informatie) kan in gesproken of geschreven vorm plaatsvinden.
- Wees voorzichtig met wat je deelt, met wie je informatie deelt en hoe je dit doet.
- Houd rekening met de aard van je gesprek en zorg voor een geschikte omgeving; voer geen vertrouwelijk gesprek in een openbare ruimte.
- Bespreek alleen zakelijke en/of vertrouwelijke zaken in een aparte ruimte of verplaats de vergadering naar een locatie die beter geschikt is.
- Neem altijd je persoonlijke spullen mee.
- Deel alleen informatie wanneer dit strikt noodzakelijk is, zowel binnen als buiten de organisatie.



4 Ken de risico's van e-mail, internet en sociale media

- Gebruik e-mail en internet verantwoord.
- Gebruik alleen vertrouwde sites om documenten en andere bestanden te downloaden.
- Wees je bewust van de dataclassificatie en hoe gegevens te behandelen voordat je vertrouwelijke/gevoelige informatie verstuurt.
- Controleer of e-mails afkomstig zijn van vertrouwde e-mailadressen.
- Ga voorzichtig om met e-mails en bijlagen van onbekende herkomst.
- Probeer de genoemde service en website via internet te bereiken in plaats van rechtstreeks via de link in de e-mail of tekst; of ' zweef ' boven de link om te controleren of deze daadwerkelijk doorverwijst naar de genoemde website.
- Markeer e-mails met mogelijke bedreigingen en meld deze bij jouw IT-/beveiligingsafdeling.
- Plaats geen gevoelige informatie over de organisatie of klanten op sociale media.
- Houd werk en privé gescheiden. Gebruik bijvoorbeeld één sociaal mediakanaal alleen voor privédoeleinden en het andere voor zakelijke doeleinden.

5 Ga zorgvuldig om met mobiele apparatuur

- Stel een pincode of wachtwoord in op je apparaat, inclusief jouw voicemail.
- Vergrendel je apparaat wanneer je het niet gebruikt.
- Volg de richtlijnen van de organisatie bij het opslaan en bewerken van informatie.
- Houd mobiele apparaten altijd in het zicht en laat ze nooit achter in de auto.
- Gebruik alleen beveiligde netwerken en versleutel informatie wanneer je onderweg bent.

6 Houd je werkomgeving veilig

- Communicatie (en het delen van informatie) kan in gesproken of geschreven vorm plaatsvinden.
- Wees voorzichtig met wat je deelt, met wie je informatie deelt en hoe je dit doet.
- Houd rekening met de aard van je gesprek en zorg voor een geschikte omgeving; voer geen vertrouwelijk gesprek in een openbare ruimte.
- Bespreek alleen zakelijke en/of vertrouwelijke zaken in een aparte ruimte of verplaats de vergadering naar een locatie die beter geschikt is.
- Neem altijd je persoonlijke spullen mee.
- Deel alleen informatie wanneer dit strikt noodzakelijk is, zowel binnen als buiten de organisatie.

7 Bescherm jouw wachtwoorden

- Geef je wachtwoord nooit aan iemand anders! Aan niemand, zelfs niet aan een collega of familielid.
- Praat nooit over een wachtwoord in het bijzijn van anderen.
- Geef geen hints over de structuur van je wachtwoord (bijvoorbeeld 'mijn achternaam').
- Geef tijdens jouw vakantie je wachtwoord niet aan collega's.
- Als iemand om een wachtwoord vraagt, verwijs hen dan naar deze wachtwoordtips en -trucs.
- Gebruik de functie 'Wachtwoord onthouden' niet binnen applicaties en browsers – gebruik in plaats daarvan een wachtwoordmanager.
- Wijzig je wachtwoord als je wordt geïnformeerd dat jouw account of wachtwoord mogelijk is gelekt.
- Activeer 2FA / MFA waar mogelijk. 2FA is een specifiek type multifactor-authenticatie (MFA) dat de toegangsbeveiliging versterkt door twee methoden (ook wel authenticatiefactoren genoemd) te vereisen om je identiteit te verifiëren.
- Gebruik nooit hetzelfde wachtwoord voor meerdere accounts; maak unieke wachtwoorden.

8 Meld informatiebeveiligings-incidenten

- Houd je mobiele apparatuur bij je.
- Laat je apparatuur nooit onbeheerd achter.
- Vergrendel je computer wanneer je jouw werkplek verlaat.
- Gebruik hoezen, cases of skins om jouw apparatuur te beschermen.
- Jouw toegangspas, wachtwoorden, pincodes en sleutels zijn alleen voor jou bedoeld; deel deze niet met anderen.
- Beveilig je apparatuur met een wachtwoord, pincode of biometrische gegevens en gebruik waar mogelijk multifactor-authenticatie.
- Zorg ervoor dat je computer en applicaties zo snel mogelijk worden bijgewerkt.
- Beveilig je e-mail met 2FA / MFA. Verzoeken tot het resetten van jouw wachtwoord van veel services komen in je e-mail terecht. Toegang tot je e-mail betekent toegang tot veel services.



Meer informatie

Wil je meer weten over onze security-diensten? Neem een kijkje op onze website. Je kunt hier eveneens informatie aanvragen over onze Vulnerability Scan. Wij adviseren je graag over de mogelijkheden en voorwaarden.