7 Vuistregels voor informatiebeveiliging

Informatiebeveiliging onder controle

Accountancy Gemak Software Gemak

An Exact Company

Alles onder controle

7 Vuistregels voor informatiebeveiliging

1 Ga zorgvuldig om met informatie

- Vergrendel je computer wanneer je je werkplek verlaat.
- Houd je werkplek en (vergaderruimte) netjes.
- Berg je spullen op in een la of ruimte die op slot kan of gooi ze op een correcte manier weg (shredder, afgesloten bak).
- Sluit alle apparatuur volledig af voor je het kantoor verlaat om te voorkomen dat je informatie verliest.
- Neem je persoonlijke bezittingen altijd mee.
- Deel vertrouwelijke bedrijfsinformatie of bestanden alleen via beveiligde kanalen.
- Wees je ervan bewust met wie je informatie deelt.
- Controleer de inhoud en de ontvanger(s) van je e-mails voordat je ze verstuurt.
- Voorkom dat anderen vertrouwelijke informatie op je scherm kunnen zien.
- Houd rekening met de aard van je activiteiten en werk in een passende omgeving; een vertrouwelijk gesprek voer je dus niet in een openbare ruimte.

2 Ga veilig om met je wachtwoord en computer

- Houd je mobiele apparatuur bij je.
- Laat je apparatuur niet zomaar onbewaakt achter.
- Gebruik covers, cases of skins om je apparatuur te beschermen.
- Je toegangskaart, wachtwoorden, pincodes en sleutels zijn alleen voor jou bestemd, dus leen ze niet uit aan anderen.
- Bescherm je apparatuur met een wachtwoord, pincode of biometrische gegevens en gebruik waar mogelijk multi-factor authenticatie.
- Wijzig wachtwoorden volgens het wachtwoordbeleid.
- Gebruik voor elk account een ander wachtwoord. Gebruik bijvoorbeeld niet hetzelfde wachtwoord voor Facebook als voor je zakelijke e-mail.

3 Communiceer met de nodige voorzichtigheid

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

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

- Ga verantwoord om met e-mail en internet.
- Gebruik alleen betrouwbare sites voor het downloaden van documenten en andere bestanden.
- Wees je bewust van de dataclassificatie en hoe je moet omgaan met data alvorens vertrouwelijke/ gevoelige informatie te verzenden.
- Controleer of e-mails afkomstig zijn van betrouwbare e-mailadressen.
- Ga voorzichtig om met e-mails en bijlages van onbekende herkomst.
- Zweef boven een link (klik er NIET op) om te controleren of de link daadwerkelijk doorverwijst naar de genoemde website.
- Markeer e-mails met potentiële dreigingen en stel de IT Supportdesk hiervan op de hoogte.
- Plaats geen gevoelige informatie over de organisatie of klanten op social media.
- Houd werk en privé gescheiden. Gebruik bijvoorbeeld het ene socialmediakanaal alleen privé, en het andere voor zakelijke doeleinden.

5 Ga zorgvuldig om met mobiele apparatuur

- Stel een pincode of wachtwoord in op je apparaat, ook voor je voicemail.
- Vergrendel je apparaat als het niet in gebruik is.
- Volg de richtlijnen van de organisatie bij het opslaan en bewerken van informatie.
- Houd mobiele apparaten altijd in zicht en laat ze nooit in de auto liggen, ook niet in de kofferbak.
- Gebruik alleen beveiligde netwerken en versleutel informatie als je onderweg bent.

6 Houd je werkomgeving veilig

- Stel de receptie op de hoogte van bezoekers.
- Begeleid je bezoekers en laat eventuele bezoekerspassen zichtbaar dragen.
- Draag je toegangspas zichtbaar.
- Let op onbekende bezoekers, mensen die alleen rondlopen en/ of verdachte personen zonder toegangspas. Vraag of je ze naar de receptie of hun contactpersoon kunt brengen.

7 Meld informatie-beveiligingsincidenten

- Incidenten met betrekking tot informatiebeveiliging en privacy moeten meteen gemeld worden. Het doet niet ter zake of je er zelf bij betrokken bent of er alleen getuige van bent.
- Meld informatiebeveiliging- en privacyincidenten bij je leidinggevende en een Information Security Officer.
- Als je niet zeker weet waar en hoe je incidenten moet melden, aarzel dan niet om bij je collega's of manager te informeren hoe je op de juiste manier een informatiebeveiliging- en privacyincident kan melden.
- Raadpleeg informatiebeveiligingprocedures en werkinstructies regelmatig op wijzigingen. Deze kun je vinden op het intranet.

Accountancygemak.nl

E info@accountancygemak.nl
T +31 184 44 44 44

Softwaregemak.nl

E info@softwaregemak.nl
T +31 184 44 44 44