INFORMATIEBEVEILIGING: DAT DOE JE GEWOON ZELF!

BEWUST OMGAAN MET INFORMATIE IS BELANGRIJK VOOR HET SUCCES VAN ONS BEDRIJF EN ONZE KLANTEN. JIJ SPEELT DAARBIJ EEN BELANGRIJKE ROL! VEEL KUN JE NAMELIJK GEWOON ZELF DOEN ALS HET OM INFORMATIEBEVEILIGING GAAT. OF JE NU VANUIT KANTOOR, VANUIT JE BUS, IN DE CLOUD OF THUIS WERKT – JE KUNT INFORMATIE VEILIG DELEN, VEILIG OPSLAAN EN ZORGEN VOOR VEILIGE TOEGANG.

Ook weten wat je zelf kunt doen? Lees hieronder waar je met informatiebeveiliging te maken hebt. Kijk op de achterzijde voor de volledige omschrijving.

IN DE CLOUD
Wachtwoorden, e-mail, versleutelen documenten en apps.

THUIS
Veilige verbinding, Intune en social media.

IN DE BUS (ONDERWEG)
Openbare verbindingen, bedrijfswagen en zakelijke telefoon en tablet vergrendelen.

OP KANTOOR
Toegang, veilig printen, bezoek en clean desk.

een Koninklijke VolkerWessels onderneming

INFORMATIEBEVEILIGING, ALLES OP EEN RIJTJE:

IN DE CLOUD

- Wees altijd alert op het delen van (bedrijfsgevoelige) informatie.
- Gebruik een wachtwoord van voldoende lengte en verschillende schrijftekens en verander het regelmatig, ook wanneer dit niet wordt afgedwongen.
- Deel je wachtwoorden nooit met anderen.
- Klik nooit zomaar op een link in een e-mail en controleer altijd het e-mailadres van de afzender. Vertrouw je de e-mail niet? Verwijder deze dan uit je inbox.
- Open nooit bijlagen van onbekende personen.
- Ga je een e-mail versturen? Controleer dan vóór verzending of de geadresseerden juist zijn.
- Versleutel en verstuur bestanden met gevoelige gegevens met de tools die daarvoor beschikbaar zijn, bijvoorbeeld VolkerWessels transfer.
- Download op je werktelefoon alleen apps vanuit de store (Google/Apple) die veilig zijn. Bij twijfel neem contact op met de service desk. Wees daarnaast terughoudend met het gebruik van niet zakelijke apps.
- Gebruik alleen Cloudapplicaties die als veilig zijn geclassificeerd. Als je het niet zeker weet vraag dit dan na bij de Contactpersoon Privacy en Informatiebeveiliging (CPIB) van je werkmaatschappij.

THUIS

- Beveilig je thuisnetwerk (WiFi) met een zelfgekozen wachtwoord.
- Gooi thuis geen bedrijfsdocumenten weg, doe dit op kantoor.
- Deel nooit je BSN, bankgegevens of andere vertrouwelijke persoonsinformatie.
- Gebruik social media alleen op persoonlijke titel.
- Werk met een beveiligde internetverbinding, heb je een onveilige internetverbinding gebruik dan VPN.
- Maak gebruik van Intune als je een privé telefoon hebt voor zakelijke doeleinden.

IN DE BUS (ONDERWEG)

- Gebruik geen openbare WiFi (voor zakelijke doeleinden), tenzij je een VPN verbinding tot stand kunt brengen.
- Sluit je bedrijfswagen of auto af en laat niets in het zicht liggen.
- Neem digitale gegevensdragers (laptop, smartphone) altijd mee.
- Zorg dat je telefoon en tablet automatisch worden vergrendeld na maximaal 5 minuten.

OP KANTOOR

- Weet wie je binnen laat. Spreek iemand gerust aan als je twijfelt.
- Blijf bij de printer tijdens het printen, ook als het papier op is of er een storing is.
- Lock je scherm wanneer je wegloopt, dit kan gemakkelijk met Windows toets + L.
- Voer geen vertrouwelijk gesprek op de gang.
- Maak een whiteboard/flipover leeg na gebruik.
- Maak je bureau leeg voor vertrek.
- Sluit kasten af.
- Gooi oude bedrijfsdocumenten in de afgesloten papiercontainer.
- Geef vertrouwelijke en geheime documenten een label. Geef dit ook aan als je een dergelijk document deelt.
- Versleutel vertrouwelijke documenten met een wachtwoord. Als je het versleutelde Zip-bestand stuurt naar een collega of contactpersoon: stuur het wachtwoord gescheiden via sms of WhatsApp.
- Sluit applicaties af op je computer wanneer je deze niet meer gebruikt.