Informatiebeveiliging en Privacy

VolkerWessels

Inhoudsopgave

Informatiebeveiliging en Privacy

Steeds vaker bevinden we ons online. Op onze laptop, tablet of mobiel. Dit brengt gevaren met zich mee. Cybercriminaliteit neemt nog steeds toe. Denk hierbij bijvoorbeeld aan het ontvangen van phishing e-mails en virussen op je computer of verlies van (privacy) gevoelige informatie.

Om ons bedrijf voor deze risico's te beschermen is een informatiebeveiliging- en privacybeleid opgesteld. In deze documenten staat beschreven hoe VolkerWessels haar bedrijfsinformatie en persoonsgegevens beschermt.

Informatiebeveiligingsbeleid

Bij informatiebeveiliging (IB) gaat het om het beschermen van alle informatie waarvan is vastgesteld dat deze een belangrijke waarde vertegenwoordigt voor VolkerWessels. Het is daarom essentieel dat informatie in onze systemen vertrouwelijk en beschikbaar zijn en integer blijven. Om dat voor elkaar te krijgen hebben we een set van maatregelen opgesteld die we goed onderhouden en regelmatig controleren.

"Samen werk maken van Informatiebeveiliging en Privacy"

Privacybeleid

In het privacybeleid is uitgewerkt hoe je op de juiste manier omgaat met persoonsgegevens en op welke manier wij kunnen aantonen welke persoonsgegevens wij als organisatie verwerken en waarom. Hiermee zorgen we er ook voor dat we de privacywetgeving (Algemene Verordening Gegevensbescherming, AVG) naleven.

Belangrijkste aandachtspunten hierin zijn dat:

- persoonsgegevens alleen verwerkt mogen worden wanneer wij hiervoor een doel en een grondslag hebben;
- persoonsgegevens alleen verwerkt mogen worden die noodzakelijk zijn voor het doel;
- wij goed omgaan met persoonsgegevens en deze beveiligen conform ons informatiebeveiligingsbeleid;
- wij alle verwerkingen van persoonsgegevens vastleggen in een register.

Iedereen is verantwoordelijk voor de veilige omgang met bedrijfsinformatie en persoonsgegevens. VolkerWessels zorgt voor een goed beveiligde werkplek, maar we kunnen dit niet zonder hulp van jou. Voor jou als medewerker is het belangrijk je te houden aan de 11 gouden regels. Wat dit in de praktijk betekent, wordt uitgelegd in dit boekje.

VolkerWessels

SAMEN WERK MAKEN VAN INFORMATIEBEVEILIGING EN PRIVACY

11 gouden regels

1. Weet wie wat mag zien

- Deel informatie niet zomaar met iedereen.
- Werk je in de trein of op een andere publieke locatie, wees dan voorzichtig met ‘meelezers’ en ‘toehoorders’.
- Denk goed na welke informatie je ophangt in je kantoorruimte of in de keet.
- Bedenk goed welke mensen toegang moeten hebben tot welke bedrijfsinformatie.

“Eerst denken, dan doen!”

2. Berg vertrouwelijke documenten op

- Zorg dat je documenten met vertrouwelijke informatie (bedrijfsgevoelige informatie maar ook informatie over personen) goed opbergt.
- Laat documenten niet rondslingeren en berg deze zorgvuldig op in bijvoorbeeld een afgesloten kast.
- Wacht tijdens het printen en haal (gevoelige) informatie direct van de printer.
- Zorg voor een opgeruimd bureau en sluit je kasten en lades af.

“Opgeruimd staat netjes”

3. Deel bestanden veilig

- Stuur bestanden met vertrouwelijke informatie niet onbeveiligd naar de ontvanger.
- Gebruik geen USB-sticks of andere datadragers voor het delen van informatie zonder overleg met jouw ICT-afdeling.
- Deel bestanden via SharePoint/Teams/OneDrive of via VolkerWessels Transfer (https://volkerwesselstransfer.nl).

“Niet mailen, maar delen”

4. Vergrendel je scherm

- Zit je niet achter je pc of laptop? Zorg dat je je scherm vergrendelt als je wegloopt (). zodat anderen niet bij jouw e-mail of bestanden kunnen.
- Zorg ook voor schermvergrendeling op je andere mobiele apparaten zoals een telefoon of een tablet met bijvoorbeeld een pincode of vingerafdruk.

“Check je werkplek”

5. Maak je wachtwoorden sterk en uniek en houd ze geheim

- Kies sterke en unieke wachtwoorden, denk hierbij aan een wachtwoordzin.
- Deel je wachtwoord nooit met anderen.
- Gebruik onze wachtwoordmanager ‘Keeper’ om op een veilige en makkelijke manier wachtwoorden te generen en te bewaren.
- Gebruik geen zakelijke wachtwoorden voor privédoeleinden.

“Behandel je wachtwoorden als de sleutels van je huis, laat ze niet rondslingeren”

6. Bescherm je apparaten

- Laat je laptop, tablet of telefoon nooit onbeheerd achter, ook niet in je bus of auto. Criminelen kunnen met scanners zien of er een apparaat in een auto ligt.
- Zorg dat je de meest recente updates op al je mobiele apparaten installeert zodat de beveiliging up-to-date is.
- Download zelf geen software op je bedrijfsapparaat.
- Geef opvolging aan waarschuwingen van je virusscanner door ondersteuning te vragen bij de ICT-Servicedesk.

“Houd criminaliteit op afstand”

7. Wees alert op verdachte personen, e-mail en telefoontjes

- Meld bezoekers aan en begeleid deze binnen het pand of op het project.
- Wees alert op onbekende personen die je ziet rondlopen in een kantoor, project of keet.
- Let goed op verdachte e-mails: phishing e-mail komt steeds vaker voor. Klik niet op links of bijlagen in een e-mail die je niet vertrouwt.
- Wees alert op telefoontjes van onbekende nummers en WhatsApp- en sms-fraude.

"Hang op, klik weg en meld het bij het Meldpunt VolkerWessels"

8. Meld een incident direct

Denk je dat er iets niet in orde is of ben je bang dat er sprake is van een informatiebeveiligingsincident of een datalek? Meld dit dan direct bij meldpunt@volkerwessels.com, ook buiten kantoortijden en op zon- en feestdagen.

Voorbeelden wanneer je iets moet melden:

- verlies laptop, telefoon of document;
- klikken op link of openen bijlage van phishing e-mail;
- virusinfectie op je computer;
- social media bericht met vertrouwelijke informatie;
- telefonisch doorgeven vertrouwelijke of geheime gegevens;
- versturen document naar verkeerd (huis)adres;
- open deur die op slot dient te zijn;
- versturen e-mail naar verkeerde ontvanger;
- e-mail met grote hoeveelheid collega's in de CC in plaats van BCC;
- verlies klantgegevens (zoals tekening over infrastructuur van klant).

"Wie meldt is een held"

9. Gebruik persoonsgegevens alleen voor het doel waarvoor je ze hebt verzameld

Wanneer je persoonsgegevens vraagt, bijvoorbeeld voor een sollicitatie of registratie op een projectlocatie, mag je deze gegevens niet zomaar voor een ander doel gebruiken.

"Weet welke persoonsgegevens je waarvoor mag gebruiken"

10. Verzamel en bewaar alleen persoonsgegevens die je echt nodig hebt

Soms moet je voor jouw werkzaamheden bepaalde persoonsgegevens opvragen/verzamelen. Let op: je mag alleen die gegevens opvragen en bewaren die je echt nodig hebt.

"Verwerk niet meer persoonsgegevens dan noodzakelijk"

11. Vernietig persoonsgegevens veilig wanneer je ze niet meer nodig hebt – check eerst de bewaartermijnen

- Heb je de opgevraagde/bewaarde persoonsgegevens niet meer nodig? Check dan wat de bewaartermijn van die gegevens zijn (zie Archiveringsbeleid VolkerWessels).
- Zorg dat je persoonsgegevens die je niet meer nodig hebt aan het eind van de bewaartermijn op veilige wijze vernietigt.

"Wat je niet hebt, hoef je niet te beveiligen"

Vertrouwelijke informatie: wat is dat?

Binnen VolkerWessels kijken we op drie manieren naar informatie.

- Beschikbaarheid - De informatie is beschikbaar en toegankelijk.
- Integriteit - De informatie is juist en actueel.
- Vertrouwelijkheid - De informatie is alleen toegankelijk voor de juiste personen.

Hieronder wordt toegelicht wat vertrouwelijkheid verder inhoudt. De mate van vertrouwelijkheid is verdeeld in 4 niveaus.

0. Openbaar - Openbare informatie mag door iedereen worden gezien.
1. Intern - Interne informatie is alleen toegankelijk voor medewerkers (eigen en inhuur) en indien nodig externen.
2. Vertrouwelijk - Vertrouwelijke informatie is toegankelijk voor een beperkte groep mensen. Voorbeelden hiervan zijn persoonsgegevens, klantgegevens en financiële rapportages.
3. Strikt vertrouwelijk - Strikt vertrouwelijke informatie is alleen toegankelijk voor een zeer beperkte groep mensen. Voorbeelden zijn bijzondere persoonsgegevens of zeer gevoelige bedrijfsinformatie.

Een verdere uitwerking wat dit in de praktijk betekent vind je terug in de richtlijn ‘Omgang met (vertrouwelijke) documenten en e-mail’

Phishing e-mail

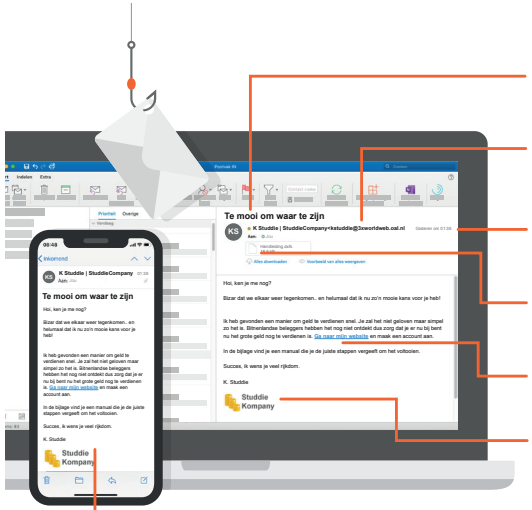
Phishing komt veelvuldig voor. Het is belangrijk dat wij hier allemaal alert op zijn.

Hiernaast wordt uitgelegd waar je op moet letten en hoe je een phishing e-mail kunt herkennen.

VolkerWessels

WORD GEEN SLACHTOFFER VAN PHISHING E-MAILS!

TIPS OM PHISHING E-MAIL TE HERKENNEN



Heb je een phishing e-mail ontvangen? Ook al heb je niet op de link geklikt, meld dit dan direct bij meldpunt@volkerwessels.com of bel naar 088 186 1120.

Hoe sneller je meldt, hoe sneller het meldpunt actie kan ondernemen in het beschermen van jouw en andere accounts en onze bedrijfsinformatie.

Actief op social media? Wees alert!

De mooiste verhalen over VolkerWessels lezen, dat willen we allemaal wel. En wie kunnen ons deze beter vertellen dan de medewerkers zelf? VolkerWessels laat jou daarom graag op social media communiceren over je werk. Zodra je gebruik maakt van social media om te communiceren over je werk gelden een aantal uitgangspunten waar je rekening mee moet houden.

1. Openbaarheid - Wees je ervan bewust dat alles wat je op social media plaatst openbaar is.
2. Eigen verantwoordelijkheid - Denk voor publicatie na over de mogelijke gevolgen van je communicatie. Herstel eventuele fouten.
3. Respectvol en integer - Publiceer altijd respectvol en positief.
4. Persoonlijke titel - Schrijf in de ik-vorm en nooit namens VolkerWessels of haar ondernemingen.
5. Vertrouwelijke informatie - Zet vertrouwelijke en gevoelige informatie over VolkerWessels en/of haar ondernemingen nooit online.
6. Woordvoering en persbeleid - Wek nooit de indruk dat je een officiële mededeling van VolkerWessels naar buiten brengt.
7. Aanmaken social media account - Gebruik alleen een privé e-mailadres voor registratie op social media.
8. Auteursrecht/toestemming - Gebruik geen materiaal van anderen zonder toestemming en maak eventuele bronnen zichtbaar. Publiceer geen herkenbare foto's van personen zonder toestemming.

Geef het door

Neem altijd contact op met jouw directie, de afdeling communicatie van jouw onderneming of de afdeling concern communicatie wanneer:

- je twijfelt of je iets kunt publiceren;
- je online een uiting ziet die wat jou betreft niet past binnen de richtlijnen van VolkerWessels;
- je benaderd wordt (bijvoorbeeld door een journalist) voor informatie ten behoeve van een publicatie;
- je online een bericht ziet dat schadelijk kan zijn voor VolkerWessels en/of haar ondernemingen.

Vragen of opmerkingen:
communicatie@volkerwessels.com

Meld vermoedens van misstanden bij de Vertrouwenslijn:
0800 0222 931 | Toegangscode: 07681

Notities

Checklist

Als ik de ‘11 gouden regels’ toepas, dan geldt voor mijn werkplek het volgende:

Mijn werkplek op kantoor of in de keet

- ☐ Mijn bureau is opgeruimd en leeg.
- ☐ Ik vergrendel mijn computer/tablet als ik van mijn werkplek ga (+ L).
- ☐ Vertrouwelijke documenten en persoonsgegevens zijn veilig opgeborgen of, als ik ze niet meer nodig heb, heb ik ze vernietigd of verwijderd.
- ☐ Ik heb mijn wachtwoorden veilig in ‘Keeper’ staan en nergens meer opgeschreven.
- ☐ Ik gebruik geen USB-sticks en andere mobiele datadragers.
- ☐ Voor het versturen van (privacy) gevoelige informatie gebruik ik VolkerWessels Transfer of de chatfunctie van Teams.
- ☐ Ben ik niet aanwezig dan heb ik mijn laptop, tablet en/of telefoon op een veilige afgesloten plek opgeborgen.
- ☐ Mijn kast(en) en bureauladen zijn dicht en/of op slot.
- ☐ Deuren zijn op slot waar nodig.

Wanneer ik bezoek ontvang

- ☐ Mijn bezoeker is aangemeld en ingeschreven.
- ☐ Ik haal mijn bezoek op en begeleid deze weer terug naar de receptie.

In de bedrijfswagen/auto

- ☐ Ik laat geen vertrouwelijke informatie achter in mijn auto.
- ☐ Mijn laptop, telefoon en tablet laat ik niet in de auto liggen (ook niet in de achterbak).

Notities

Voor meer informatie over hiervoor genoemde onderwerpen kun je contact opnemen met de contactpersoon informatiebeveiliging en/of privacy van jouw werkmaatschappij.

Meld beveiligingsincidenten en datalekken zo spoedig mogelijk, ook bij twijfel!

Stuur een mail naar **meldpunt@volkerwessels.com**

VolkerWessels