Naam document
Beveiligingsbeleid Twan Caldenhoven PMT

Versienummer
1.0

Versiedatum
5 juni 2020

Beveiligingsbeleid Twan Caldenhoven PMT

Inleiding
Dit document geeft de algemene beleidsuitgangspunten in het kader van privacy weer en is een aanvulling op de technische en organisatorische maatregelen die getroffen dienen te worden in het kader van de Algemene Verordening Gegevensbescherming (AVG).

Door middel van dit document kan **Twan Caldenhoven PMT** verdere in- en aanvulling geven op het door haar te voeren privacy beleid, grip houden op privacy risico's en de medewerkers handvatten bieden op het gebied van normen met betrekking tot het beveiligen van gevoelige bedrijfsinformatie.

Beveiligingsbeleid
In ons beveiligingsbeleid gebruiken wij een aantal definities. Deze definities kunnen in enkelvoud en meervoud worden gebruikt.

Beleid: dit beveiligingsbeleid.
Bedrijfsapparatuur: apparatuur zoals laptops, PC's en mobiele telefoons in eigendom van **Twan Caldenhoven PMT** en in gebruik bij de medewerker of het eigendom van de medewerker, maar o.a. in gebruik voor werkzaamheden.

Doel van het beveiligingsbeleid
De normen binnen **Twan Caldenhoven PMT** vaststellen op het gebied van technische en organisatorische beveiligingsmaatregelen.

Scope van het beveiligingsbeleid
De scope van dit beleid omvat alle bedrijfsprocessen binnen **Twan Caldenhoven PMT**, onderliggende informatiesystemen, informatie en externe partijen en het gebruik daarvan door medewerkers.

Het beleid is van toepassing op alle bij **Twan Caldenhoven PMT** werkzame (interne en externe) medewerkers en bestuurder(s). Hieronder wordt verstaan: zowel het personeel als de niet in loondienst werkende personen of ingehuurde arbeidskrachten.

- Dit beveiligingsbeleid is van toepassing op alle offline en online systemen die bezit zijn van **Twan Caldenhoven PMT**, worden gebruikt door **Twan Caldenhoven PMT** en waar **Twan Caldenhoven PMT** controle over heeft;
- De informatie in de werkingssfeer van dit beleid: informatie die is opgeslagen, gedeeld met en/of verzonden is door **Twan Caldenhoven PMT** en gereproduceerd kan worden op telefoon, laptop etc.

Mobiele (privé)apparatuur en thuiswerkplek
Twan Caldenhoven PMT biedt haar medewerkers de mogelijkheid om gebruik te maken van bedrijfs- en privé-apparaten zoals laptops en telefoons. Twan Caldenhoven PMT behoudt het recht om het gebruik van bedrijfsapparaten eenzijdig in te trekken wanneer blijkt dat de normen omtrent dit beleid niet na worden geleefd door een medewerker.

- De beveiligingsmaatregelen binnen dit beleid hebben betrekking op zowel door **Twan Caldenhoven PMT** verstrekte middelen als privé-apparatuur ('bring your own device' (BYOD)). Op privé-apparatuur en bedrijfsapparatuur waarmee verbinding wordt gemaakt met het bedrijfsnetwerk van **Twan Caldenhoven PMT**, is **Twan Caldenhoven PMT** bevoegd om beveiligingsinstellingen af te dwingen die tenminste, maar niet beperkt tot, zien op de volgende zaken:

- Controle op wachtwoord;
- Encryptie van communicatie;
- Het opsporen en tegenhouden van malware;
- Het opsporen tegenhouden van virussen.

- Op verzoek van **Twan Caldenhoven PMT** dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan zoals: 'virusscanners'. De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van bedrijfsinformatie van het bedrijfsnetwerk en de bedrijfsintegriteit van **Twan Caldenhoven PMT**.

- Informatievoorzieningen en mobiele telecommunicatie applicaties zoals o.a.: 'Whatsapp' alsook sociale netwerken zoals 'Facebook', 'Twitter' etc. zijn door het lage beschermingsniveau niet geschikt voor het delen van vertrouwelijke informatie en daarom verboden voor het delen van bedrijfsinformatie in welke vorm dan ook.

Gebruik van bedrijfs- en privé-apparatuur
Twan Caldenhoven PMT acht gelimiteerd acceptabel persoonlijk gebruik tijdens werkuren als redelijk zolang dit de belangen van **Twan Caldenhoven PMT** o.a. op het terrein van dit beveiligingsbeleid niet schaadt.

Bedrijfs- en privéapparaten zoals telefoons of laptops, mogen echter niet gebruikt worden voor:
- het opslaan, uitzenden, overdragen of overbrengen van aanstootgevend materiaal;
- deelnemen in bedrijfsactiviteiten anders dan **Twan Caldenhoven PMT**.

Gebruikmaken van bedrijfs- en privé-apparatuur, zoals een zakelijke telefoon of laptop, op een andere plek dan op kantoor is toegestaan indien:
- De veiligheid van het te gebruiken netwerk voldoet aan veiligheidseisen gesteld in dit document;
- Geen verbinding wordt gemaakt met een 'open netwerk';
- Indien dit noodzakelijk is voor het uitvoeren van de werkzaamheden voor **Twan Caldenhoven PMT**.

Verdere verplichtingen voor medewerkers Twan Caldenhoven PMT
Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan binnen 24 uur melding te maken bij de directeur van **Twan Caldenhoven PMT**.

- Medewerkers maken bij voorkeur geen gebruik van USB-sticks of andere gegevensdragers in de werkomgeving of voor zakelijk gebruik en proberen dit in uitzonderingsgevallen te reduceren tot nihil. Dit helpt ons om datalekken te voorkomen.

Wachtwoorden/wachtzinnen
Voor alle werknemers en/of freelancers is toegang tot werkzaamheden voor **Twan Caldenhoven PMT** beveiligd met een wachtwoord.

Veiligheid en datalekken
• Om dataverlies tegen te gaan dient minimaal één keer per maand een back-up te worden gemaakt van de essentiële bedrijfsgegevens binnen **Twan Caldenhoven PMT** zodat de continuïteit kan worden gegarandeerd. Dit back-up materiaal dient opgeslagen te worden in de cloud van **Twan Caldenhoven PMT**. Deze back-up dient te worden bewaard onder beveiligde omstandigheden en toegang tot deze back-up mag enkel worden vrijgegeven door de directeur van **Twan Caldenhoven PMT**;

Vernietiging van vertrouwelijke informatie

Om datalekken en ongeautoriseerde toegang tot bedrijfsinformatie te voorkomen zal alle stoffelijke informatie binnen **Twan Caldenhoven PMT** dat geen doel meer heeft binnen **Twan Caldenhoven PMT** en persoonsgegevens bevat, worden vernietigd conform de bewaartermijn gesteld in het privacyreglement.

Derden
Het is verboden om derden toegang te verlenen tot het bedrijfsnetwerk van **Twan Caldenhoven PMT**, tenzij:

- Toestemming voor toegang tot het bedrijfsnetwerk schriftelijk wordt gegeven door de directeur;
- Een wettelijk voorschrift dat verplicht;
- Dat nodig is in het kader van de overeenkomst.

Toegang tot het pand

- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe;
- De uitgifte van toegangsmiddelen tot het kantoorpand wordt geregistreerd;
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de hoogste standaard;
- Indien gebruik gemaakt wordt van beeldmateriaal wordt dit beperkt door de Algemene Verordening Gegevensbescherming en nadere regels;
- De fysieke toegang tot ruimten waar zich informatie en ICT-voorzieningen bevinden is voorbehouden aan bevoegd personeel;

Einde dienstverband
Zodra een medewerker/freelancer Twan Caldenhoven PMT permanent verlaat, worden accounts verwijderd of ontoegankelijk gemaakt.

Aanspreken van onbekende personen
Indien een medewerker een voor hem/haar onbekende persoon in het kantoorgebouw van **Twan Caldenhoven PMT** treft, spreekt de medewerker/freelancer deze persoon aan, stelt zichzelf voor en vraagt de persoon in kwestie wat hij/zij hier doet. Personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Het is de taak van de medewerker om hen beleefd maar duidelijk de weg naar de uitgang van het gebouw te wijzen en ze daar naartoe te begeleiden.