



VCK Travel wil op het gebied van informatievoorziening- en beveiliging alle belanghebbenden; medewerkers, klanten en leveranciers, vertrouwen en zekerheid geven over de zorgvuldige manier waarop informatie wordt verwerkt, opgeslagen en geraadpleegd. Wij willen ons onderscheiden door de mate en de wijze waarop wij omgaan met de bescherming van privacy gevoelige gegevens. Het beleid is er om die reden op gericht om een zo veilig mogelijke omgeving te creëren, zowel bij toepassingen die wij in eigen beheer onderhouden als bij het gebruik van cloud toepassingen.

Wij hebben te maken met externe bedreigingen, maar ook interne risico's doordat steeds meer gegevensstromen worden verwerkt en gekoppeld. Keuzes tussen transparantie en openheid van informatie enerzijds en beveiliging van vertrouwelijke informatie anderzijds vergen zorgvuldige afweging. De komende jaren blijft VCK Travel zich inzetten op het verhogen van informatieveiligheid, bescherming van de privacy en verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie.

Voor de beheersing van de informatiebeveiliging en de bescherming van de privacy is een informatiemanagementsysteem ingericht en geïmplementeerd in de gehele VCK Travel organisatie op alle kantoren. Dit managementsysteem is gecertificeerd volgens de ISO 27001 norm voor informatiebeveiliging, ISO 27701 norm voor privacy en ISO 22301 norm voor bedrijfscontinuïteit. De Data Protection Officer heeft de verantwoordelijkheid en de taak om dit managementsysteem te onderhouden en continu te verbeteren. Ons beleid voor informatiebeveiliging is van toepassing op de gehele organisatie en geldt voor alle managers en medewerkers van VCK Travel. Het informatiebeveiligingsbeleid van VCK Travel is in lijn met de relevante landelijke en Europese wet- en regelgeving.

Het MT speelt een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Zo maakt het MT een inschatting van het belang dat de verschillende delen van de informatievoorziening voor VCK Travel hebben, de (privacy) risico's die VCK Travel hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het MT dit beleid voor informatiebeveiliging op, de Data Protection Officer draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan. VCK Travel heeft een samenhangend pakket van maatregelen ter waarborging van de betrouwbaarheid van het informatievoorzieningsproces getroffen en zal dit onderhouden.

Medewerkers worden periodiek op verschillende manieren bewust gemaakt van de risico's op het gebied van informatiebeveiliging, worden op de hoogte gebracht van het nieuwe beleid voor informatiebeveiliging en ontvangen instructie om in hun werkzaamheden goed vorm te kunnen geven aan de normen die het beleid stelt.

Wij spannen ons in om de risico's op de informatiebeveiliging en privacy van onze bedrijfsactiviteiten zoveel mogelijk te voorkomen of te reduceren en het informatiebeveiligingssysteem continu te verbeteren, door de volgende doelstellingen:

### **Uitgangspunten**

De uitgangspunten van ons informatiebeveiligingsbeleid zijn:

- De kern van onze bedrijfsactiviteiten betreft het verwerken van data. Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor VCK Travel. De verantwoordelijkheid voor informatiebeveiliging ligt bij de managers,

met het MT als eindverantwoordelijke. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.

- VCK Travel beperkt het verzamelen en verwerken van persoonsgegevens tot een minimum dat relevant, proportioneel en nodig is voor de geïdentificeerde doeleinden.
- Er is een privacy policy opgesteld waarin o.a. informatie over de verwerkingen, de rechten van de betrokkenen en het delen van informatie is opgenomen. Deze privacy policy is gepubliceerd op alle websites van VCK Travel.
- VCK Travel wil voorkomen dat data gelekt wordt en dat er oneigenlijk gebruik van informatie wordt gemaakt.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd.
- Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses.
- Jaarlijks worden concrete doelstellingen, acties en maatregelen afgesproken. Middelen die nodig zijn om deze doelstellingen te bereiken worden door de directie beoordeeld en indien goedgekeurd ter beschikking gesteld.
- De Data Protection Officer ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.
- VCK Travel stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.
- Het informatiebeveiligingsbeleid van VCK Travel is in lijn met de relevante landelijke en Europese wet- en regelgeving en voldoet daarnaast aan vrijwillig onderschreven eisen.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid worden vastgesteld en vastgelegd.
- Bij onverhoopte datalekken treedt het Protocol datalekken in werking en indien van toepassing wordt melding gemaakt bij de Autoriteit Persoonsgegevens.
- Alle medewerkers van VCK Travel hebben een eigen verantwoordelijkheid ten aanzien van informatiebeveiliging. Zij worden geïnformeerd over en getraind in het omgaan en gebruik van beveiligingsprocedures.
- VCK Travel wil zeker stellen dat informatie uitsluitend toegankelijk is voor diegenen die daartoe geautoriseerd zijn. Iedere medewerker, zowel vast als tijdelijk, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

## **Informatiebeveiligingssysteem**

VCK Travel heeft een managementsysteem volgens de ISO 27001, ISO 27701 en ISO 22031 normen opgesteld in de vorm van een handboek. Dit handboek is op het intranet gepubliceerd en vanuit efficiency- en milieuoogpunt alleen digitaal beschikbaar.

Het managementsysteem wordt d.m.v. presentaties, workshops en artikelen op de kantoren en afdelingen aan alle medewerkers toegelicht. De leveranciers worden door de verantwoordelijke collega's geïnformeerd over het informatiebeveiligings- en privacybeleid van VCK Travel.