statuut informatiebeveiliging

1 Inleiding

De directie onderkent dat het toenemende gebruik van datacommunicatiemogelijkheden (zoals internet, thuiswerken, video-vergaderen, digitale facturatie), de massaliteit van de dagelijkse communicatie met heel diverse organisatie- en project-betrokkenen, de omvang van de bestanden, en de toenemende professionalisering van de computercriminaliteit, tot een grotere afhankelijkheid en kwetsbaarheid van de informatievoorziening leiden.

De risico's die hiermee samenhangen zijn zeer aanzienlijk en kunnen een bedreiging vormen voor de vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening en daarmee indirect voor ons imago en dus onze continuïteit. Daarom is, naast dit statuut informatiebeveiliging, een e-mail, internet, telewerk en bedrijfsmiddelenbeleid opgesteld. Dit beleid maakt integraal onderdeel uit van het Statuut informatiebeveiliging.

Gelet op de mogelijke impact van verstoringen op de continuïteit berust de eindverantwoordelijkheid voor het beleid inzake de beveiliging en de interne controle van de geautomatiseerde informatievoorziening bij de directie.

Dit Statuut maakt deel uit van ons algehele beveiligingsbeleid. De doelstelling van het Statuut inzake de vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening luidt:

"Het zorgen voor een raamwerk van beleidsuitgangspunten met betrekking tot de exclusiviteit, integriteit en beschikbaarheid van de geautomatiseerde informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld wordt, teneinde de geautomatiseerde informatievoorziening te beschermen tegen interne en externe bedreigingen."

Alle leidinggevenden dienen ervoor zorg te dragen dat aan de in dit Statuut geformuleerde beleidsuitgangspunten wordt voldaan bij de inrichting van de organisatie, procedures, werkwijze en de daarbij gehanteerde informatiesystemen.

Algemene regel is dat we hierin risicomijdend is. Maar onder druk van het tijdig leveren van kwaliteit aan onze klanten kan dit principe af en toe in de steek gelaten worden.

Bij de realisatie van de doelstellingen mag nooit uit het oog worden verloren dat het geheel van maatregelen samenhangend moet zijn, hanteerbaar is en blijft, het werkplezier niet onnodig wordt aangetast en dat de (sociale) controle vanzelfsprekend is en op eenvoudige wijze gerealiseerd kan worden.

2 Risico-afhandelingsplan

In ons managementsysteem zijn de risico's te identificeren door alle risico's met Middel (oranje) of Hoog (rood) risico te filteren. De getroffen, te treffen en wel geïdentificeerde, maar (nog) niet ingevoerde beheersmaatregelen om de risico's terug te brengen tot een aanvaardbaar niveau, zijn hierin eveneens opgenomen. Op risico's die als "Laag" geclassificeerd zijn is geen verder actie noodzakelijk. Indien bij herbeoordeling blijkt dat de classificatie van een Laag-risico is verslechterd naar Midden of Hoog, dan wordt dit risico opgenomen in het Risico-afhandelingsplan.

Restrisico's zijn resterende risico's met een score van "Middel" of "Hoog" na alle reeds genomen maatregelen ter beperking van de risico's. Zie voor uitleg omtrent de Risicoanalyse ook ons organisatiehandboek.

In het Risico-afhandelingsplan (Risk Mitigation Plan) worden de restrisico's opgenomen, waar nog beheersmaatregelen op toegepast moeten worden om het restrisico terug te brengen tot het gewenste niveau. Dit kunnen beheersmaatregelen zijn als genoemd in de Annex A van de ISO 27001:2005 norm, maar ook eigen gekozen beheersmaatregelen. Indien aanvullende beheersmaatregelen noodzakelijk zijn (rood), dan worden hiervoor acties gepland in het Risico-afhandelingsplan en wordt hieraan een eigenaar toegewezen, die verantwoordelijk is voor de aanpak van het risico.

De restrisico's worden door ondertekening van dit Statuut door de directie uitdrukkelijk aanvaard. Hierbij wordt als voorwaarde gesteld dat voor de restrisico's, voor zover mogelijk, een plan van aanpak (Risico-afhandelingsplan) wordt vastgesteld om restrisico's beheersbaar en aanvaardbaar te maken.

3 Beleid m.b.t. IB

De missie is sterk gericht op de kwaliteit van dienstverlening, omdat onze activiteiten schadegevoelig zijn voor de leefomgeving. Verwerkingen die niet aan de eisen en wensen van klanten voldoen(incidenten), kunnen voor zowel onze klanten als voor andere betrokkenen nadelige gevolgen hebben.

De belangen van onze klanten hebben betrekking op de beschikbaarheid, betrouwbaarheid en integriteit van informatie. Daarom zorgen wij ervoor dat alle haar toevertrouwde informatie op de juiste manier verwerkt wordt en onder de juiste voorwaarden beschikbaar is voor alleen de geautoriseerde verwerkers en (eind)gebruikers.

Informatie die onder onze verantwoordelijkheid wordt verwerkt en de hiervoor gebruikte systemen worden, voor zover relevant, beveiligd tegen de risico's van misbruik en onbedoeld gebruik.

Dit wil zeggen:
- onder **informatie** worden alle gegeven verstaan, die middels fysieke of digitale dragers worden verwerkt en van betekenis zijn voor de opdrachtgever of andere betrokken partijen. Deze informatie is geclassificeerd in 3 groepen, te weten:
  - **Vertrouwelijk.** Hieronder vallen alle data van klanten, waarin persoonsgegevens zijn opgenomen. Toegang tot deze data is beperkt tot alleen die medewerkers, die deze data uit hoofde van hun functie moeten verwerken. Alle data die niet expliciet als Intern of Publiek is aangemerkt, wordt geacht vertrouwelijk te zijn.
  - **Intern.** Deze klasse omvat alle overige data van klanten en bedrijfsgegevens van onszelf. Toegang tot deze data is beperkt tot onze medewerkers.
  - **Publiek.** Dit bevat alle overige data, welke iedereen mag weten en welke ook op andere manieren vrij beschikbaar is. Toegang tot deze data is niet beperkt.
- onder de juiste manier van verwerking wordt hier de verwerkingsmethode verstaan die wij met onze opdrachtgevers zijn overeengekomen. Deze methode voorziet in een maximalisatie van efficiënt en effectief gebruik van de informatie met in achtneming van eventuele risico's.
- **geautoriseerde verwerkers** zijn medewerkers, die op basis van hun functieomschrijving worden aangewezen om de informatie te verwerken.
- de **gebruikers** van de informatie zijn onze opdrachtgever en eventueel de klanten van onze opdrachtgever. Wij zorgen ervoor, voor zover dat binnen haar macht ligt, dat de informatie bij de juiste eindgebruiker of bij de opdrachtgever terecht komt.
- onder misbruik en onbedoeld gebruik worden alle handelingen verstaan die door onze medewerkers of organisaties en individuen daarbuiten worden uitgevoerd zonder dat zij daartoe geautoriseerd zij door de verantwoordelijken binnen onze organisatie en/of onze opdrachtgever, of handelingen die in strijd zijn met de geldende Wet- en regelgeving op het gebied van informatie en informatie verwerking. De risico's hierbij bestaan uit de kans en de omvang van de schade die de betrokkenen door misbruik of onbedoeld gebruik kunnen lijden.

De fysieke en logische beveiliging van onze bedrijfsgebouwen is zodanig, dat de vertrouwelijkheid, integriteit, beschikbaarheid en continuïteit van de gegevens en gegevensverwerking gewaarborgd is.

Aanschaf, installatie en onderhoud van geautomatiseerd gegevensverwerkende systemen, alsmede inpassing van nieuwe technologieën, mag geen afbreuk doen aan het niveau van de veiligheid van de geautomatiseerde informatievoorziening en dient altijd gemeld te worden aan onze KAM-functionaris, die tevens optreedt als CBP.

Opdrachten aan derden voor het uitvoeren van werkzaamheden worden omgeven met maatregelen die waarborgen dat er geen inbreuk op de vertrouwelijkheid, integriteit, beschikbaarheid en continuïteit van de geautomatiseerde informatievoorziening kan ontstaan. Deze maatregelen zijn opgenomen in het organisatiehandboek.

Er zijn voorzieningen aanwezig om de vertrouwelijkheid, integriteit, beschikbaarheid en continuïteit van de geautomatiseerde systemen te kunnen vaststellen en waarborgen.

Logische toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot onze geautomatiseerde systemen, gegevensbestanden en programmatuur.

Datatransport is zodanig met de beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid, integriteit van de gegevens en de informatievoorziening als geheel.

Teneinde computervirusinfecties te voorkomen wordt slechts gewerkt met geautoriseerde versies van programmatuur.

Het beheer en de opslag van gegevens is zodanig dat geen informatie verloren kan gaan.

De verwerking en het gebruik van gegevens is onderworpen aan de actuele wet- en regelgeving. De betreffende kennis van wet en regelgeving is aanwezig en wordt continue aangevuld.

Bij thuiswerkers die gebruik maken van een VPN-verbinding worden alle handelingen verricht op ons interne netwerk. Deze gebruikers hebben geen data op hun privé systeem staan en zijn akkoord gegaan met het e-mail, internet, telewerk en bedrijfsmiddelenbeleid.

Het kan zijn dat een werknemer van de werkgever een laptop, smartphone, tablet of enig ander device aangeboden krijgt. Op deze devices kan de bedrijfsgerelateerde data staan zowel e-mail, internet, telewerk en bedrijfsmiddelenbeleid.

Alle informatie en documentatie dient te worden geclassificeerd overeenkomstig de betreffende procedure in ons organisatiehandboek, zoals verwoord in de gedragsregels verderop in dit document (Clean Desk Policy).

Elke medewerker is op de hoogte gesteld van het door onze organisatie gevoerde informatiebeveiligingsbeleid en wordt geacht zich hieraan te houden. Alle beleidsdocumenten zijn gepubliceerd in de kantine en op het netwerk.

Ondertekening directie.

Door ondertekening geeft de directie te kennen dat de in dit document genoemde normen en regels door haar worden erkend als basis voor het te voeren beleid in de praktijk en als richtlijn om concrete beheersmaatregelen in te voeren.

Straatmakersbedrijf H.C. Koot BV
Utrecht, 02-02-2023

J. Koot
directeur