1 Over dit informatiseringsbeveilingsbeleid

1.1 Doel, toepassingsgebied en gebruikers

Dit beleid is gericht op het definiëren van het doel, de richting, de principes en de basisregels voor Informatiebeveiliging.

Dit beleid is van toepassing op het toepassingsgebied (de scope) van het Managementsysteem voor Informatiebeveiliging zoals bepaald in dit beleid. Gebruikers van dit document zijn zowel alle werknemers van de organisatie, als ook de relevante externe partijen.

Als tien security vinden we dat elke organisatie moet streven naar een tien voor security. Wij zien het dan ook als onze taak en plicht om (MKB-)organisatie te helpen tegen Cyberincidenten en zo hun, maar ook onze (digitale) wereld veiliger te maken. Dat kunnen we met technische middelen, maar dat kan niet zonder het volgen van een bepaald plan of, in dit geval, een informatiebeveiligingsbeleid.

Om onze klanten, partners en relaties verwachten dat wij expert zijn op diverse vlakken van Cybersecurity, dat wij kunnen zorgen dat informatie van hen veilig blijft. We willen inderdaad borgen en aantonen dat wij veilig omgaan met klantgegevens, bedrijfsgeheimen en interne documenten. Hoe kunnen wij als Cybersecurity dienstverlener serieus genomen worden als wij niet aantoonbaar met informatiebeveiliging kunnen omgaan?

1.2 Waarom

Dit beleid is een doorvertaling van onze ambities om een onderneming te zijn die actief bijdraagt aan een betere en veilige wereld. Om deze ambities te halen, maar ook om het continue toetsen van de regels en normen die we daarbij (behoren te) hanteren, maken we bij tien security gebruik van een ISMS, een Information Security Managent Systeem.

Dit helpt ons, en daarbij ook onze klanten en relaties, om vertrouwelijk informatie beter te beveiligen, werkprocessen te borgen en te voldoen aan relevante wet- en regelgeving. Wij begrijpen namelijk dat onze klanten en relaties blind vertrouwen op ons als Security dienstverlener.

Als tien security vinden we dat we een bepaalde verantwoordelijkheid hebben naar onze klanten en relaties; wij willen aantoonbaar laten zien dat we, door het inzetten van een ISMS:

- werken volgens bepaalde procedures (structuur, periodiek overleg vanuit ISMS, periodieke risico-analyses);
- continue werken aan het verbeteren van onze organisatie en daarbij behorende beveiliging. Het ISMS zal voldoen aan de van toepassing zijnde wet- en regelgeving;
- anticiperen op bedreigingen kansen van buitenaf en op die manier Informatiebeveiliging up-to-date houden;
- regelmatige monitoring en evaluatie van onze beveiligingsmaatregelen om te voldoen aan de eisen van de ISO27001;

Een en ander is uitgewerkt in het document "ISMS Handboek”. Dit ISMS stelt ons, tien security, in staat om risico's te minimaliseren, compliant te zijn met (internationale) normen en de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen.

1.3 Geldigheid en documentbeheer

Dit document is geldig vanaf de definitieve versie datum. De eigenaar van dit document is de directie van de organisatie. Deze dient het document minstens één keer per jaar te beoordelen en indien nodig bij te werken.

1.4 Goedkeuring van dit beleid

Hierbij bevestigt de directie de geldigheid van dit informatiebeveiligingsbeleid.

‘s-Graveland, 31 januari 2023
Namens tien security:
Abram Schermer, Algemeen Directeur