Directie- en beleidsverklaring

De Directie hecht grote waarde aan een goede kwaliteit van de te leveren goederen en diensten, evenals aan het zorgvuldig omgaan met data en gegevens van belanghebbenden. Om dit inzichtelijk te maken en te borgen is ervoor gekozen om dit - mede - met behulp van de ISO 9001 en ISO 27001 norm te realiseren.

De ISO-certificeringen kunnen gebruikt worden als bewijsvoering richting klanten en partners inzake de commitment voor het borgen van de kwaliteit van dienstverlening en het beschermen van privacy en data. De ISO-certificeringen kunnen tevens als marketing argument benut worden.

De directie heeft als uitgangspunt het bedrijf primair in te richten op klanten waarmee een SLA-overeenkomst is gesloten. Hiervoor is gekozen om de kwaliteit van de dienstverlening gericht te kunnen verhogen en SLA-klanten optimaal te bedienen. Dit moet leiden tot een dienstverlening waarbij de organisatie de partij is die in alle lagen van de klant een toegevoegde waarde kan leveren als ICT dienstverlener.

De directie ziet erop toe dat het beleid, de visie en de onderliggende processen en procedures in praktijk worden gebracht en op alle niveaus begrepen en op peil gehouden wordt. Middels een jaarlijkse directiebeoordeling/ evaluatie van het complete managementsysteem, waarin de doeltreffendheid wordt gemeten en nieuwe doelstellingen worden geformuleerd, wordt bewerkstelligd dat er een continue verbetering plaatsvindt. De directie voert daarnaast maatregelen door die de doeltreffendheid van het managementsysteem verbeteren.

Beleidsuitgangspunten Informatiebeveiliging

Definitie

Collabite heeft én verwerkt informatie van klanten, particulieren, medewerkers, partners en leveranciers uitsluitend met betrekking tot de eigen bedrijfsvoering. Informatie is een bedrijfsmiddel waar Collabite de plicht en de verantwoordelijkheid voor heeft om het te beschermen. Het waarborgen van de beschikbaarheid, integriteit en confidentialiteit van informatie en daarmee het voorkomen van misbruik, is van essentieel belang bij het leveren van diensten en producten. Mocht informatie gebruikt worden voor activiteiten buiten de eigen bedrijfsvoering wordt hier eerst schriftelijk toestemming voor gevraagd aan de informatie-eigenaar, alvorens de informatie wordt gedeeld.

De organisatie zorgt ervoor dat:

- Confidentialiteit: informatie is alleen beschikbaar voor geautoriseerde personen
- Integriteit: zorgen voor juistheid en compleetheid van informatie
- Beschikbaarheid: geautoriseerde personen hebben toegang tot relevante informatie wanneer nodig
- Binnen het bedrijf een actuele en complete risico-inventarisatie aanwezig is, welke periodiek en bij interne of externe wijzigingen wordt bijgewerkt
- Voldoen aan actieve naleving op de van toepassing zijnde wet- en regelgeving, voorschriften, standaarden en contractuele verplichtingen
- Proactief en adequaat reageren op informatiebeveiligingsincidenten en risico's en het toepassen van veiligheidsmaatregelen om het restrisico terug te brengen naar het acceptabele niveau
- Informatiebeveiliging wordt actief en doorlopend uitgedragen en beleefd binnen de organisatie doormiddel van leiding, scholing en awareness training of andere activiteiten.
- Tijd, geld en middelen beschikbaar zijn gesteld

- Binnen Collabite wordt gewerkt met o.a. persoonsgegevens van klanten en apparatuur van derden. Collabite gaat met deze eigendommen zeer zorgvuldig om tijdens beheer en gebruik.

Reikwijdte

Het beleid, standaarden, processen en procedures, beschreven in het managementsysteem, zijn van toepassing op alle medewerkers, maar ook op: leveranciers, opdrachtnemers/uitzendkrachten en alle andere gecontracteerde derde partijen die toegang hebben tot de informatie of informatiesystemen van Collabite. Het beleid is van toepassing op alle vormen van informatie:

- Spraak, “face to face” of medegedeeld per telefoon
- Hardcopy gegevens, afgedrukt of geschreven op papier
- Informatie die is opgeslagen in geautomatiseerde bestanden
- Communicatie per post / koerier, fax, e-mail
- Opgeslagen en verwerkt via de servers, pc’s, laptops, mobiele telefoons, pda's,
- Opgeslagen op elk type verwijderbare media, cd's, dvd’s, tape, usb-sticks, digitale camera's

Verantwoordelijkheden

Algemeen

Van alle medewerkers wordt verwacht dat zij een proactieve houding hebben ten aanzien van Informatiebeveiliging. Dat houdt in:

- Verantwoord omgaan met- en adequaat beschermen van gevoelige informatie in overeenstemming met de daarvoor opgestelde bedrijfsregels,
- Melden van beveiligingsrisico’s, incidenten en/of misbruik via het meldingsformulier.

Rollen

Rollen De volgende medewerkers hebben een rol in het kwaliteits- en informatiebeveiligings-team en zijn door de directie bevoegd om de werkzaamheden gerelateerd aan deze rollen uit te voeren.

- Kwaliteit en Information Security Manager: Peter Fleurkens
- Kwaliteit coördinator: Jolanda van Berkel
- Security officer: Erik Noort

Nalevingsbeleid

Het bewust of onbewust niet naleven van het beleid en/of onderliggende processen en procedures door een medewerker kan resulteren in disciplinaire maatregelen tegen de desbetreffende medewerker.

Bodegraven, 7 januari 2025

Aldus vastgesteld door de Directie,

De heer A. Middelveld, Algemeen Directeur ----------

De heer S. Kluin, Business unit Directeur ----------

De heer P. Fleurkens, Operationeel Directeur ----------