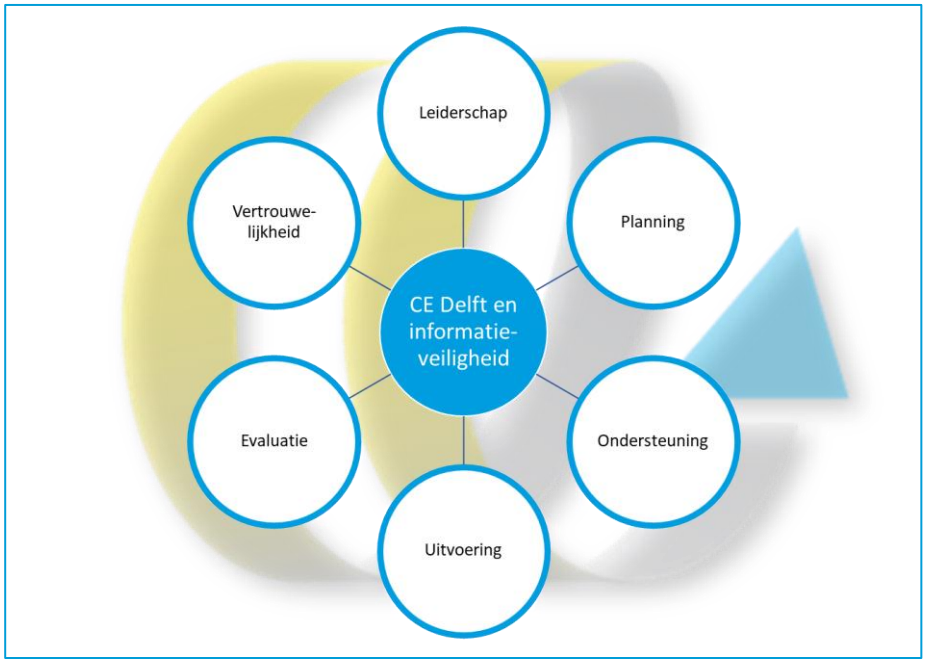
1 Informatieveiligheid

CE Delft werkt voor heel verschillende organisaties; enerzijds grote multinationals en de Europese Unie, maar anderzijds ook kleine NGO's en gemeenten. Hierdoor werken wij vaak met gegevens die variëren van concurrentiegevoelige bedrijfsgegevens tot persoonsgegevens van inwoners. Wij vinden het belangrijk dat deze informatie veilig is bij CE Delft en dat onze opdrachtgevers er op kunnen vertrouwen dat hun gegevens alleen gebruikt worden waarvoor ze bedoeld zijn.
Om de veiligheid van informatie binnen CE Delft te garanderen werken wij met een systeem van dataveiligheid en vertrouwelijkheid. Dit systeem wordt hieronder toegelicht, en is ingericht conform ISO27001.

Een veilige omgeving voor informatie

Het beleid voor informatieveiligheid kent zes kernpunten. Deze worden weergegeven in de onderstaande figuur. Met de invulling van deze kernpunten sluiten wij aan bij de nieuwste normen die gangbaar zijn bij het beheren en verwerken van grote hoeveelheden vertrouwelijke informatie.



1.1 Leiderschap

Binnen CE Delft is de verantwoordelijkheid voor informatieveiligheid belegd bij de directie. De directeur Interne Organisatie is verantwoordelijk. De uitvoering van de werkzaamheden voor informatieveiligheid worden uitgevoerd door onze eigen interne Automatiserings- en informatiebeheerders (IT-afdeling). Deze medewerkers krijgen daarbij ondersteuning van de IT-dienstverlener Q-Network. Dit team, van directie tot uitvoering, werkt samen in het

realiseren van een veilige omgeving voor informatie. De verantwoordelijkheden op het gebied van informatieveiligheid van onze medewerkers zijn vastgelegd in hun functieprofiel. De verantwoordelijkheden van Q-Network zijn contractueel vastgelegd.

1.2 Planning

Er wordt gewerkt met een ICT-roadmap op korte en lange termijn. Er wordt maandelijks overleg gevoerd in het team van directeur Interne Organisatie, IT-afdeling en IT-dienstverlener. Hierbij worden de ontwikkelingen in veiligheid op systeemniveau besproken en worden afspraken gemaakt over implementatievraagstukken voor het onderhouden en verbeteren van de veiligheid. Bij deze implementatie wordt een scheiding aangebracht in een test- en productieomgeving. Dit om te voorkomen dat zowel de informatieveiligheid als het primaire proces van CE Delft ontregeld worden.

1.3 Ondersteuning

Voor de medewerkers van CE Delft is een eerste- en tweedelijnsondersteuning aanwezig. De eerstelijnsondersteuning wordt ingevuld door de interne IT-afdeling. De tweedelijns door Q-Network. Bij de ondersteuning wordt gebruik gemaakt van een ticketsysteem. Hierdoor is het mogelijk het verloop van het ondersteuningsverzoek te volgen en zorg te dragen voor een goede overdracht van de ondersteuning tussen de eerste en tweede lijn. De ondersteuning vindt plaats op zowel software als hardware(veiligheid).

1.4 Uitvoering

Om zorg te dragen voor een IT-systeem dat up to date is en voorzien is van alle benodigde, recente beveiligingen zijn de volgende maatregelen getroffen:

1. Ons centrale systeem is gebaseerd op "Server Based Computing" en is naast EDR (Endpoint Detection & Reponse) beveiligd middels multi-factor authentication en een software restriction policy.
2. Met behulp van patch management worden de systemen up to date gehouden.
3. Het datacenter waar de servers staan heeft een ISO 27001 certificering.
4. De decentrale systemen (laptops, tablets) worden hoofdzakelijk op afstand beheert en geupdate door gebruik te maken van een RMM-oplossing (remote monitoring and management). De interne IT-afdeling van CE Delft is hiermee in staat om de medewerkers optimaal te ondersteunen, op iedere locatie en op een veilige wijze. Het RMM-systeem is voorzien van 2-factor authentication, activiteiten binnen de RMM-oplossing worden vastgelegd in een (audit) logboek. Het RMM-systeem voorziet in de uitrol van updates, antivrius (EDR) en security updates (patch management).
5. Samen met het ticket systeem zorgt de RMM-oplossing voor een optimale samenwerking tussen de interne IT afdeling van CE Delft (1e lijn) en Q-network (2e lijn). Indien nodig is de interne IT-afdeling aanwezig op het kantoor van CE Delft om op locatie de benodigde handelingen uit te voeren.

Naast een up to date systeem, worden ook actieve middelen ingezet om de veiligheid te verhogen. Inloggen op de systemen gebeurt door middel van 2-factor authentication (2FA), waarbij ieder personeelslid via een persoonlijk device inlogt. Dit wordt aangevuld met afscherming van de inlogmogelijkheden op basis van geografische locatie (standaard staat deze beperkt ingesteld en locaties kunnen op verzoek (tijdelijk) worden toegevoegd).

Databestanden van CE Delft zijn beveiligd middels een back-up. Deze back-up voldoet aan de hoog aanbevolen 3-2-1 back-up strategie waarbij een back-up dus ook offline wordt bewaard. De back-up wordt dagelijkse gecontroleerd.

1.5 Evaluatie en verbeteren

CE Delft werkt aan een systeem van periodieke rapportages over de veiligheid van haar systemen. Deze rapportage vindt plaats aan de hand van de tools die door CE Delft gebruikt worden voor het beheren van de (informatie)veiligheid. Onderdeel van de evaluatie is de continue monitoring van 'high risk login'-pogingen en pogingen tot phising.
Deze rapportages worden tijdens het maandelijks overleg (zie kopje planning) besproken. Daarnaast maakt CE Delft gebruik van externe controle op de uitrol van de laatste versies van de beveiligingsupdates.
Op basis van de evaluaties wordt gekeken of en waar verbeteringen plaats kunnen en moeten vinden om de informatieveiligheid te waarborgen. Maatregelen op dit vlak worden opgenomen in de roadmap, en de benodigde budgetten hiervoor worden gereserveerd in de jaarlijkse ICT-begroting die wordt opgesteld door de Directie (Algemeen Directeur en Directeur Interne Organisatie).

1.6 Vertrouwelijkheid

Naast de veiligheid is ook de vertrouwelijkheid van informatie van belang. Hiervoor heeft CE Delft diverse niveaus aangebracht:

6. Het eerste niveau is vastgelegd in het arbeidscontract van de medewerker, waarmee alle medewerkers hebben getekend voor geheimhouding.
7. CE Delft maakt gebruik van SharePoint als documentbeheerssysteem. Indien een project vertrouwelijke informatie bevat of in het geheel vertrouwelijk is, dan wordt de toegankelijkheid tot de vertrouwelijke informatie beperkt tot alleen die medewerkers die vanuit hun functie in het project daar toegang voor nodig hebben.
8. Aanvullend hierop werken wij met persoonlijke of bedrijfsbrede geheimhoudingsverklaringen (NDA) en/of verwerkersovereenkomst, als een opdrachtgever hier om vraagt.
9. CE Delft publiceert data alleen na toestemming van de opdrachtgever.