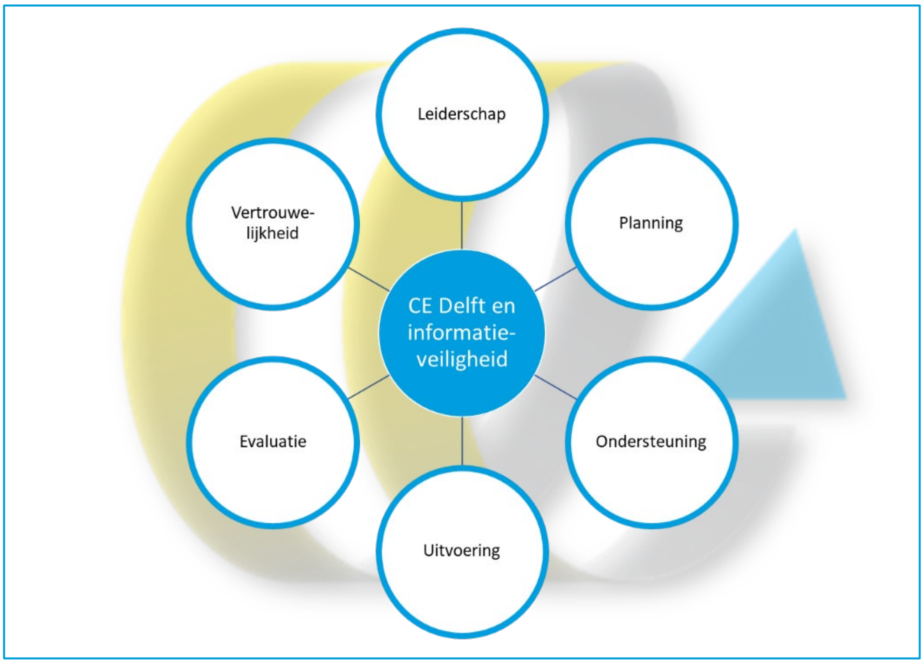
1 Informatieveiligheid

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 staan 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

De eindverantwoordelijkheid voor informatieveiligheid ligt bij de directeur Interne Organisatie. De werkzaamheden voor informatieveiligheid worden uitgevoerd door onze eigen interne Automatiserings- en informatiebeheerders (IT-afdeling). De IT-afdeling krijgt daarbij ondersteuning van onze IT-dienstverlener Q-Network. Dit team, van directie tot uitvoering, werkt samen aan een veilige omgeving voor informatie. De verantwoordelijk-heden op het gebied van informatieveiligheid van onze medewerkers zijn vastgelegd in hun functieprofiel. De verantwoordelijkheden van Q-Network zijn contractueel vastgelegd.

1.2 Planning

We werken met een ICT-roadmap op korte en lange termijn. Er is maandelijks overleg tussen de directeur Interne Organisatie, IT-afdeling en de 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 interne IT-afdeling doet de eerstelijnsondersteuning. De tweedelijns wordt door Q-Network gedaan. Bij de ondersteuning wordt gebruik gemaakt van een ticketsysteem. Hierdoor is het mogelijk het verloop van het ondersteuningsverzoek te volgen te zorgen voor een goede overdracht van de ondersteuning tussen de eerste en tweede lijn. De geldt voor zowel de software als hardware(veiligheid). De directeur Interne Organisatie is 24/7 bereikbaar voor het melden van noodsituaties (datalek, hackpogingen, etc).

1.4 Uitvoering

Om te zorgen dat het IT-systeem 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 met 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 beheerd en geupdate door gebruik te maken van een RMM-oplossing (remote monitoring and management). De IT-afdeling van CE Delft kan hierdoor de medewerkers optimaal ondersteunen, op iedere locatie en op een veilige wijze. Het RMM-systeem heeft two-factor authentication en 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 ticketsysteem zorgt de RMM-oplossing voor een optimale samenwerking tussen de interne IT afdeling van CE Delft en Q-network. De interne IT-afdeling is elke werkdag aanwezig op het kantoor van CE Delft om op locatie de benodigde handelingen uit te voeren.

Naast een up to date systeem, zijn er actieve middelen om de veiligheid te verhogen. Inloggen op de systemen gebeurt met two-factor authentication (2FA), waarbij iedere medewerker 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 worden veiliggesteld door een back-up. Deze back-up voldoet aan de hoog aanbevolen 3-2-1 back-up strategie waarbij een back-up dus ook offline en op een andere locatie wordt bewaard. De back-up wordt dagelijkse gecontroleerd.

1.5 Evaluatie en verbeteren

CE Delft werkt met een systeem van periodieke rapportages over de veiligheid van haar systemen. CE Delft gebruikt o.a. ConnectSecure voor het monitoren en beheren van deze (informatie)veiligheid. Onderdeel van de evaluatie is de continue monitoring van onder andere ‘high risk login’-pogingen, ‘risk score by assets’, ‘remediation report’ en pogingen tot phising.

High risk loginpogingen worden direct gemeld waarbij de account meteen geblokkeerd wordt. De overige rapportages (‘risk score by assets’ en ‘remediation report’) worden tijdens het maandelijks overleg (zie kopje planning) besproken en waar nodig worden de acties uit het remediation report opgepakt. Maatregelen op dit vlak worden direct genomen of opgenomen in de roadmap. De budgetten die nodig zijn worden gereserveerd in de jaarlijkse ICT-begroting die de Directie (Algemeen Directeur en Directeur Interne Organisatie) maakt.

1.6 Vertrouwelijkheid

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

1. Het eerste niveau is vastgelegd in het arbeidscontract van de medewerker, waarmee alle medewerkers hebben getekend voor geheimhouding.
2. 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.
3. Aanvullend hierop werken wij met persoonlijke of bedrijfsbrede geheimhoudingsverklaringen (NDA) en/of verwerkersovereenkomst, als een opdrachtgever hier om vraagt.
4. CE Delft publiceert data alleen na toestemming van de opdrachtgever.