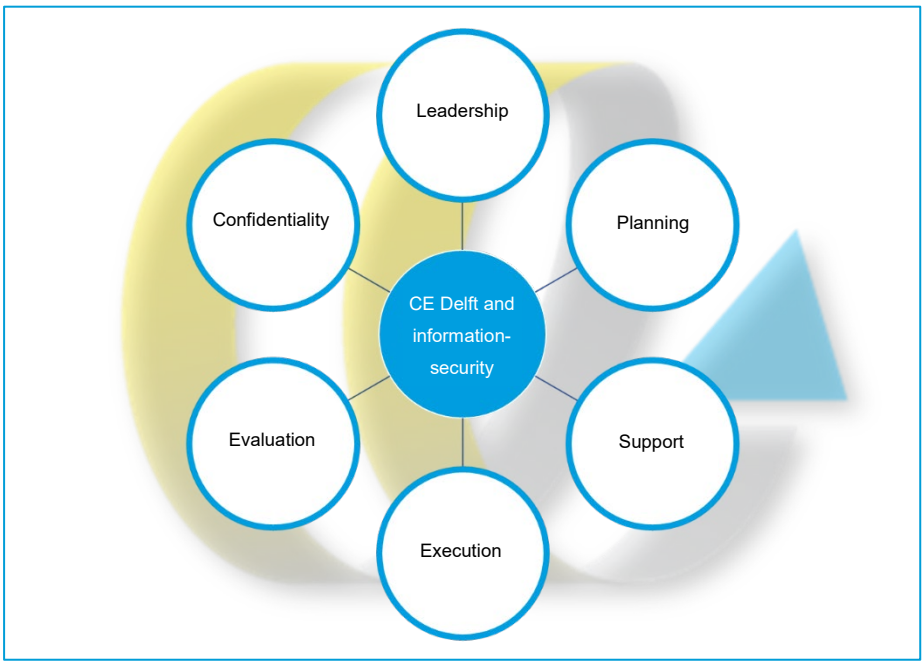
1 Information Security

CE Delft works for a wide variety of organisations; on the one hand, large multinationals and the European Union, and on the other hand also small NGOs and municipalities. As a result, we often handle data ranging from commercially sensitive business information to personal data of residents. We consider it as important that this information is kept secure at CE Delft, and that our clients can trust that their data is used solely for its intended purpose.

To ensure the security of information within CE Delft, we operate a system for data safety and confidentiality. This system is explained below and is designed in accordance with ISO27001.

A secure environment for information
The information security policy is based on six key points. These are shown in the figure below. By implementing these key points, we align with the latest standards that are common for managing and processing large volumes of confidential information.



1.1 Leadership

Final responsibility for information security lies with the Director of Internal Organisation. Tasks relating to information security are carried out by our own internal Automation and Information Managers (the IT department). The IT department is supported in this by our IT service provider, Q-Network. This team, from management to operational staff, works together to ensure a secure environment for information. The responsibilities regarding information security for our staff are detailed in their job profiles. The responsibilities of Q-Network are contractually established.

1.2 Planning

We work with an ICT roadmap for both the short and long term. There are monthly meetings between the Director of Internal Organisation, the IT department, and the IT service provider. During these meetings, developments in security at system level are discussed and agreements are made on implementation issues concerning the maintenance and improvement of security. When implementing these changes, a separation is made between a test and a production environment, to prevent both information security and the primary processes of CE Delft from being disrupted.

1.3 Support

CE Delft employees have access to both first- and second-line support. The internal IT department provides first-line support, while Q-Network handles second-line support. Support requests are managed using a ticketing system, allowing the progress of requests to be monitored and ensuring a smooth handover between first- and second-line support. This applies to both software and hardware (security). The Director of Internal Organisation is available 24/7 for reporting emergencies (such as data breaches, hacking attempts, etc.).

1.4 Execution

To ensure that the IT system is kept up to date and equipped with all necessary, recent security measures, the following actions have been taken:

1. Our central system is based on "Server Based Computing" and, in addition to EDR (Endpoint Detection & Response), it is secured with multi-factor authentication and a software restriction policy.
2. Patch management is used to keep the systems up to date.
3. The data centre where the servers are located has ISO 27001 certification.

4. The decentralised systems (laptops, tablets) are primarily managed and updated remotely by means of an RMM solution (remote monitoring and management). As a result, CE Delft's IT department can optimally support employees, at any location and in a secure manner. The RMM system uses two-factor authentication and activities within the RMM solution are recorded in an (audit) logbook. The RMM system facilitates the rollout of updates, antivirus (EDR), and security updates (patch management).
5. Together with the ticketing system, the RMM solution ensures optimal collaboration between CE Delft's internal IT department and Q-network. The internal IT department is present at the CE Delft office every working day to carry out necessary actions on site.

In addition to maintaining an up-to-date system, there are active measures in place to enhance security. Logging into the systems is done using two-factor authentication (2FA), with each employee accessing the system via a personal device. This is complemented by restricting login possibilities based on geographical location (the default setting is limited, and locations can be added temporarily upon request).

CE Delft's data files are safeguarded with a backup. This backup adheres to the highly recommended 3-2-1 backup strategy, meaning one backup is kept offline and at another location. The backup is checked daily.

1.5 Evaluation and improvement

CE Delft operates with a system of periodic reports regarding the security of its systems. CE Delft uses, among others, ConnectSecure to monitor and manage this (information) security. Part of the evaluation involves continuous monitoring of, among other things, 'high risk login' attempts, 'risk score by assets', 'remediation report' and phishing attempts.

High risk login attempts are reported immediately, and the account is instantly blocked. The other reports ('risk score by assets' and 'remediation report') are discussed during the monthly meeting (see the planning section), and actions from the remediation report are addressed where necessary. Measures in this area are taken immediately or included in the roadmap. The required budgets are reserved in the annual ICT budget prepared by the Management (General Director and Director of Internal Organisation).

1.6 Confidentiality

In addition to security, the confidentiality of information is also important. To ensure this, CE Delft has implemented several levels:

1. The first level is established in the employee's employment contract, in which all employees have signed for confidentiality.

2. CE Delft uses SharePoint as its document management system. If a project contains confidential information or is confidential in its entirety, access to the confidential information is restricted to only those employees who require access by virtue of their position in the project.
3. Additionally, we work with personal or company-wide non-disclosure agreements (NDAs) and/or data processing agreements, if requested by the client.
4. CE Delft only publishes data after receiving the client's permission.