How to start working with digital responsibility

We have listed 5 steps for how you can start with digital responsibility.

1. Do inventory of your information

Identify the information you store, transport and process which thereby needs protection. Information security encompasses the entire organisation´s operations and all information, regardless if it is in computers or on a piece of paper. Start mapping routines and processes, who has access to information and systems, and the state of your security thinking.

2. Involve management

Start involving your management and board in discussions about, and reflections on, your current Digital Responsibility position. The responsibility for security work always lies with management, as only management can decide not to mitigate security risks. Given how the rate of cyberattacks are accelerating, a decision not to invest in information security means that both the organisation and its management take a large financial risk.

3. Start acting on regulations

A part of taking digital responsibility is to follow laws and regulations that are aimed at protecting sensitive information. For example, you have to adapt to GDPR. GDPR brings revolutionary changes in IT systems. It also involves major efforts to adapt all the systems and procedures to the new requirements.

You might also have to adapt to the NIS Directive - The NIS Directive tightens the requirements for information security in terms of integrity and availability. It is important to take people, processes and technology into account to ensure information security in the affected organisations.

4. Inform stakeholders

Be clear in your communication to your customers whose data you manage on how you will protect their information. This especially applies to work with personal information as stated in GDPR.

5. Think privacy by design

It will be cheaper for those who are designing for privacy from the beginning (privacy by design). Whoever designs without understanding these impacts will need to be correct in hindsight - something that will always be more expensive than doing it correctly from the start. Therefore, expertise in the field of information security is crucial to success.

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED