

FONTAIN



INFORMATION SECURITY POLICY

Fontain is committed to safeguard the confidentiality, integrity and availability of all physical and electronic information assets of the company to ensure that regulatory, operational and contractual requirements are fulfilled. The overall goals for information security at Fontain are the following:

- Ensure compliance with current laws, regulations and guidelines, e.g. GDPR.
- Comply with requirements for confidentiality, integrity and availability for Fontain's employees, customers and stakeholders.
- Establish controls for protecting Fontain's information and information systems against theft, abuse and other forms of harm and loss.
- Motivate administrators and employees to maintain the responsibility for, ownership of and knowledge about information security, in order to minimise the risk of security incidents.
- Ensure that Fontain is capable of continuing their services even if major security incidents occur.
- Ensure the protection of personal data (privacy) and the data of clients and stakeholders.
- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by Fontain.
- Ensure that external service providers comply with Fontain's information security needs and requirements.
- Ensure flexibility and an acceptable level of security for accessing information systems remotely.

Fontain's current business strategy and framework for risk management are the guidelines for identifying, assessing, evaluating and controlling information related risks through establishing and maintaining the information security policy. Every user of Fontain's information systems shall comply with this information security policy. Violation of this policy and of relevant security requirements will therefore constitute a breach of trust between the user and Fontain and may have consequences for employment or contractual relationships.