Group Policy Information and IT Security

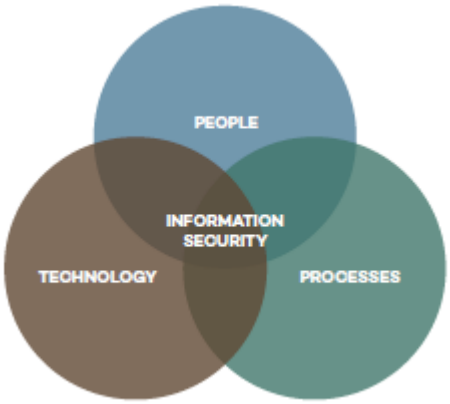
Purpose

This Information and IT Security Policy describes management's commitment to information security and its governance within AFRY. It is defined in accordance with the ISO/IEC 27001 standard on Information Security Management Systems (ISMS) and applies to all employees, contractors, and other parties with access to information owned or managed by AFRY AB.

Policy

Foundation

The foundation of AFRY's information security comprises three pillars:



Our **people** are knowledgeable, security aware and able to resist cyber-threats. They are aware of the importance of right-sizing security using risk-based decision-making.

We use **technology** to support and guide the secure use of our information assets and to implement controls to minimise risk.

Our **processes** allow our team players to securely collaborate cross-functionally, while also providing the insights required for continuous improvement.

These three pillars support a sustainable security culture that enables us to weather disruptions which might otherwise pose a threat to our customers' trust.

Information and Cybersecurity

Information and data are strategic resources for AFRY and critical to our competitiveness. This valuable information must therefore be protected from unauthorized disclosure (confidentiality) and unwanted change (integrity), while also being available when needed (availability). AFRY information security is driven by best practice principles such as least privilege, minimising data exposure, and zero trust.

AFRY is committed to maintaining a high level of security awareness within the organisation, as we are committed to maintaining the security of both our information assets and those entrusted to us.

AFRY requires that all employees familiarise themselves with all principles established by this policy, the associated directives, and mandatory information security trainings; for accepting those principles; and for acting in accordance with them.

Management system

The Information Security Management System (ISMS) is part of the AFRY Management System and specifies how to work systematically with information security risks. The ISMS is documented in the Information Security Framework, which comprises this Policy as well as other guidelines governing the secure and acceptable use of information and IT equipment.

In detailing the different aspects of working securely, the Framework considers:

— Regulatory, business, and customer demands

— The value and sensitivity of information

— The threat landscape

Roles and responsibilities

Information security is a general business responsibility that demands engagement from all parts of the organisation:

Group Executive Management is responsible for providing the aim and ambitions for information security as well as the adequate resources required to achieve the set ambitions.

The CISO is responsible for continually assessing the cyber and information security risks and challenges facing AFRY and, based on those assessments, define the strategic goals and concomitant policies. These policies are the base for the Information Security Framework.

Group IT is responsible for managing and maintaining secure IT services and solutions for all parts of AFRY in accordance with the Framework; for providing support related to these services and solutions; and for augmenting the Framework as needed for continuous improvement.

Divisions and Group Functions are responsible for implementing the Framework in their organisations. Among the requirements included in the Framework are the designation of i) roles for data governance, such as owners for all Division/Group information assets and ii) roles tasked with the creation and maintenance of division-specific information security processes and documentation.

Information owners are responsible for assessing the business value, criticality, and sensitivity of their information. This includes ensuring that any applicable regulatory requirements for their information are documented and met.

Managers are responsible for ensuring that they themselves and their staff are aware of and implement the Information Security Framework, and that they act to minimise information security risks.

All users are responsible for actively contributing to the security culture by managing information security in accordance with good practice and the Framework. This responsibility includes classifying information according to business value and reporting incidents or events that may cause information to be breached.

Any individual employee or other party that intentionally or through neglect fails to comply with the policy may be subject to disciplinary and legal measures.