Group Policy Information- and IT Security

Purpose

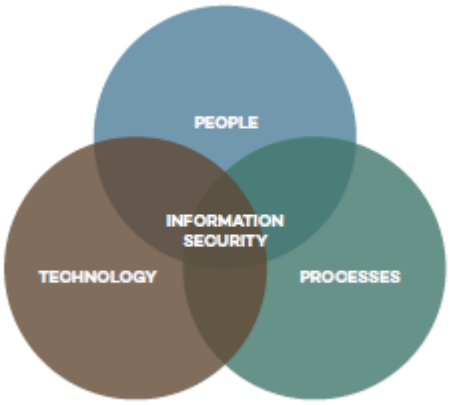
This Information- and IT Security Policy describes management's commitment to information security and how it shall be governed within AFRY. This policy is defined in accordance with the international standard ISO/IEC 27001 for creating an Information Security Management System (ISMS), and applies to all employees, contractors, and other parties with access to information owned or managed by AFRY AB. Our ability to protect employees, knowledge and information is critical to our competitiveness. Information is a strategic resource for AFRY and shall be protected whether processed manually or being automated and regardless of its form and context.

It is of utmost importance for our company that sensitive information in all external and internal relationships is protected from unauthorized disclosure **(confidentiality)** and unwanted change **(integrity)** and is available when needed **(availability)**.

Policy

Foundation

The foundation of AFRYs information security comprises three pillars:



People – We shall have high security awareness and expertise, and the courage and agility to navigate new markets and opportunities.

Processes – We shall continuously improve our Management System, creating a solid foundation of prerequisites for our team players and promoting cross-functional collaboration within business processes.

Technology – We shall be devoted to engineering excellence, delivering innovative and resilient solutions that support complex business environments and protect against the known threats of tomorrow.

These three pillars guide us towards a sustainable security culture, which enables operational excellence and prevents any damage that may disrupt or pose a threat to our customers' trust in AFRY.

Information- and Cybersecurity

AFRY is committed to a high level of security awareness within the organization. Information and data utilized by AFRY employees are assets entrusted to, or owned by, AFRY. Information is a critical asset and resource as its incorrectness or unavailability could affect business competitiveness. Information security is therefore vital to ensure that information assets are properly secured.

To protect against, and even prevent, cyber-attacks, we must all take responsibility for our use of information and communications systems. We shall therefore exercise due care and use the security controls and measures established by AFRY protects our information assets from accidental or unauthorized disclosure, misuse, improper alteration, and destruction.

We shall comply with the AFRY Information Security framework and the AFRY Acceptable Use Directive, which describes the acceptable use of AFRY's information assets, such as data, devices, networks, connected services and facilities.

We have the responsibility to familiarise ourselves with the principles covered in the Information Security e-learning.

Management system

Information Security is part of the AFRY Management System. This policy and underlying framework describe three key elements of managing information security:

— Understanding the applicable regulatory, business, customer and information security requirements

— Classifying information according to its value and sensitivity

— Risk Management

The ISMS manages risk by:

— Focusing on stakeholder and customer demands.

— Enabling intelligence and business driven decisions for the correct level of security measures.

— Continuous improvements of the management system and processes.

Roles and responsibilities

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

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

Group Risk and Security is responsible for defining security requirements and strengthening cyber resilience to protect against current and emerging threats and support AFRY global strategy.

CISO is responsible for, assessing the security challenges facing AFRY, and initiatives needed to combat escalating information security risks.

Group IT is responsible for managing and maintaining secure IT services and solutions for all parts of AFRY; for providing support related to these services and solutions; and for providing general IT-related tools and guidelines applicable throughout AFRY.

Divisions and Group Functions are responsible for ensuring that there are designated owners for all information assets.

Information owners are responsible for assessing the business value, criticality and sensitivity of their information.

Managers are responsible for ensuring that they themselves and the staff assigned within their designated areas of responsibility are aware of and compliant with the AFRY Information Security Management System (ISMS), and that they contribute to a positive security culture.

All users are responsible for actively contributing to the security culture by managing information security in accordance with good practice, and in accordance with the ISMS. 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 by wilful neglect fails to comply with the policy, may be subjected to disciplinary and legal measures.