

# Group Policy Information Security and Cybersecurity

## Purpose

This policy defines AFRY's systematic approach to managing the security of information and ICT (information and communication technology) systems, aligning with international standard ISO/IEC 27001, and ensuring that all individuals consistently adhere to security principles. It applies to all employees, contractors, and any other parties who handle information and ICT systems owned or controlled by the AFRY group of companies.

## Policy

Information and ICT security is a critical foundation that AFRY relies on to deliver sustainable, high-quality products and services while maintaining client trust and ensuring long-term resilience.

It is AFRY's policy to protect the confidentiality, integrity, and availability of information and ICT systems by systematically identifying and managing risks, fulfilling legal and contractual obligations, and embedding technical and organisational security measures throughout our operations.

The Group Chief Information Security Officer (CISO) owns the Information Security Management System (ISMS). The ISMS encompasses this policy together with its associated directives, processes, procedures, and guidelines.

Strategic information security objectives are set based on risks, regulations, business needs, and stakeholder expectations. They follow a structured process in the Information Security Management System and are reviewed annually for alignment with AFRY's strategy and emerging threats.

Details on Information and ICT security, including the ISMS and current information security objectives are available via AFRY's intranet.

This policy is reviewed at least annually or whenever significant changes in the business, technology, or risk landscape occur, to ensure its ongoing suitability and effectiveness.

### Roles and responsibilities

**Individuals** must familiarise themselves with this policy and the documented Framework, complete mandatory security training, and adhere to security requirements. Managers ensure compliance within their teams.

**Information owners** manage and safeguard their information assets, including classification, risk assessment, and compliance with security and regulatory requirements.

**Divisions and Group Functions** implement the policy and Framework within their organisations, assigning roles and responsibilities and maintaining division-specific security processes and documentation.

**Group IT** ensures the security of its services and solutions and continuously improves security measures in accordance with the Framework.

**CISO** assesses security risks, defines strategic information security objectives, owns and maintains the Information Security Management System (ISMS).

**Executive Team** provides leadership, resources, and oversight to enhance AFRY's security posture and meet client and stakeholder expectations.

**AFRY's Board of Directors** approves this policy and oversees, through the Audit Committee, the Company's Information Security Management System.

Failing to comply with this policy and documented Framework can result in disciplinary and legal measures.