Group Policy Information and IT Security

Purpose

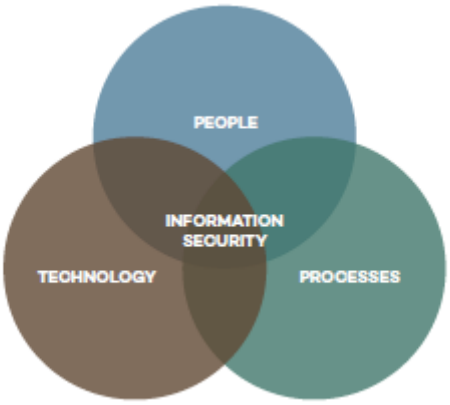
This Information and IT Security Policy describes management's commitment to information security and how it shall be governed within AFRY. This policy applies to all employees, contractors and other parties with access to information owned or managed by AFRY AB. Our ability to protect employees, knowledge 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)**, protected from unwanted change **(integrity)** and available when needed **(availability)**.

Policy

Foundation

The foundation of AFRYs information security is built on three pillars:



People – We shall have high security awareness,

how-to-knowledge and trust, to be brave and agile enough to navigate new markets and opportunities.

Processes – We shall continuously be improving our Management System and create a solid foundation of prerequisites for our team players and promote cross-functional collaboration within business processes.

Technology – We shall be devoted to engineering excellence and we apply 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 maintains the confidentiality of information entrusted to us by our clients and other parties. To succeed with this, we are committed to maintain a high security awareness and strive towards a security culture within the organization. Our commitment is presenting and protecting against cyber-attacks.

— Information, knowledge and data processed by AFRY employees, or by technological and/or physical devices, are to be seen as assets owned by AFRY.

— We shall not utilize or divulge confidential information without prior and specific authorization.

— We shall only use information's assets in accordance with our agreed upon duties and AFRY directives and guidelines.

— We shall always abide by the directives and guidelines regarding the acceptable use of AFRY's physical and virtual environment. This includes but is not limited to AFRY facilities, equipment, devices, client's facilities, network and connected service.

— We have the responsibility to stay updated with training and information.

Management system

Information Security is an integral part of the AFRY Management System. The information and IT security policy is defined in accordance with the international standard ISO/IEC 27001. The policy describes the foundation for how information security is governed within AFRY.

The governing documents describes three key elements of managing information security, these are:

— Constitutional, business and information security demands and controls for compliance.

— Information Classification.

— Risk Management.

The Information Security Management System 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:

— The Group Executive Management is responsible for providing the overall 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 managing information security according to managements ambition. Enforcing that requirements, control, and risks are managed effectively and with quality assurance. Ensuring continuous improvements and strengthening AFRYs' resilience, so to minimise risk exposure and protect against current and emerging threats.

— Corporate IT is responsible for ensuring that IT confidentiality, integrity and availability is reputable, and that IT security controls and solutions are managed and maintained within AFRY. Providing support, tools and implementation guidelines to all parts of AFRY that are dependent on IT.

— Managers are responsible for their designated area of responsibility as well as that the assigned staff within that area are aware and compliant with the AFRY Information Security Management System and contributes to a positive security culture.

— Employees are responsible for actively contributing to the security culture by being aware of how to manage information security in accordance with good practice, and in accordance with AFRY´s management system for information security. This responsibility also includes an obligation to report incidents or events that may cause information to be exposed by security breaches.

Any individual employee or other party that intentionally or by willful neglection fails to comply with the policy, may be subjected to disciplinary and legal measures.