



Our approach to Information Security



INTRODUCTION

Information Security is the practice of protecting information and related assets from unauthorised access, disclosure, alteration, destruction, or theft. It relies on the design and implementation of an Information Security Framework that provides a structured set of requirements, guidance and best practices to safeguard information in all forms - **digital, physical or spoken**.

Effective Information Security protects the organisation from a wide range of threats, prevents data breaches, supports business resilience, and strengthens the trust of customers and stakeholders.

Common Information Security threats include:

- Theft of intellectual property
- Identity theft
- Equipment theft
- Information leakage
- Sabotage
- Information extortion
- Software attacks
- Distributed Denial of Service (DDoS)

Confidentiality, Integrity and **A**vailability of Ageas information assets is being achieved by designing, implementing monitoring, reviewing and improving set of suitable controls.

SCOPE

Ageas Information Security Policy applies to **ageas SA/NV and all its Subsidiaries** and to their Staff.

For the **Subsidiaries**, should compliance with Information Security Policy result in non-compliance with local legislation or regulations, the latter must take precedence. The Group Policy owner must be informed and consulted immediately in such circumstances.

For the **Affiliates** it is recognised that the requirements of the local law, the local regulator and the majority shareholder's policy applies. However, Ageas will advise similar principles with reasonable effort.

AGEAS APPROACH TO INFORMATION SECURITY

FRAMEWORK

Ageas has designed and implemented an Information Security Management Framework, inspired by ISO/IEC 27000 series standards and ISF¹ Standard of Good Practice, to safeguard the confidentiality, integrity and availability of its information assets. The framework consists of a **strategy** document, **policy, standards**, and processes, supported by tools that ensure coherent, effective and aligned with recognised industry

¹ ISF – Information Security Forum

security practices and compliant with applicable regulatory requirements.

PROPORTIONALITY

Information Security **measures** defined in our framework are **proportionate** to the value of the information assets to be protected and designed with due consideration and documentation of the associated risks.

AWARENESS & TRAINING

Information Security is a **shared responsibility**. Ageas fosters a **security-conscious culture** through targeted thought targeted awareness, communication, training and education programmes, ensuring staff understand information-related risks and how to manage them appropriately.

EXTERNAL REVIEW

Ageas operating companies are ISO 27001:2022 certified. To maintain this certification, they undergo **yearly external assessments** conducted by accredited ISO Certification Authorities.

GOVERNANCE

Information Security roles and responsibilities are clearly defined and assigned at all levels of organisation.

The **Board of Directors** of Ageas holds **ultimate accountability** for the Information Security Policy including the design and oversight of its implementation and correct operation of the associated controls. **Day-to-day oversight** responsibility is delegated to the Ageas Group Chief Information Security Officer (**CISO**). The **Executive Committee**, together with business management, is **responsible for implementing** the Information Security Management Framework and Information Security Management System (ISMS).

Ageas has appointed a Group Chief Information Security Officer (CISO) at its head office, as well as local CISOs within its operating companies and regional offices. These CISOs are members of the Ageas Group Information Security Governance Board, which acts as:

- the governing body responsible for endorsing the Information Security Framework and overseeing the Information Security risk management process
- a platform for sharing information, best practices, and lessons learned across the Group
- a forum to identify synergies, and coordinate common initiatives

The Ageas Group CISO is responsible for developing and maintaining the Information Security Framework and supervises its implementation across the organisation. This includes:

- monitoring the effectiveness of controls
- performing yearly assessments
- overseeing information security programmes and initiatives
- reporting at least annually on Information Security risks and maturity levels to Steering and Risk Committees, Executive Management, and Board of Directors.

