**Generali Group**

# SECURITY GROUP POLICY

*Public version*


generali.com

## EXECUTIVE SUMMARY

As a major global player in the financial sector, Generali Group has important capital in terms of physical and information assets.

Generali Group is fully aware of the importance of protecting its assets from relevant threats, especially cyber threats, to maintain consumer's trust as part of Generali's core business strategy and to meet regulatory requirements. Therefore, this Policy defines a common approach for all Group Legal Entities in scope to define and guarantee a proper management of security aspects throughout the Group.

In more detail, Group Security concerns both processes and technologies and therefore it requires the implementation of technical, organizational and behavioural measures to protect and preserve Companies' assets in terms of people, information and physical assets from security threats and risks.

In this context, the Group Security Policy outlines strategies and directions to protect people, information and physical assets addressing the following topics:

- Security Mission and Strategy;
- Security Objectives;
- Security Principles;
- Security Governance;
- Security Management Process;
- Security Areas and Domain.

The mission of Group Security consists of implementing adequate security measures and processes to guarantee the protection of company assets in terms of people (travel security), information and physical assets, as well as in ensuring the security of business. Cyber Security has a dedicated focus, due to the high relevance of this topic in the Group and the increasing requirements on the topic from external regulation.

To achieve its mission and to be able to effectively manage the increasing complexity of security risks, Group Security has adopted a One-Security approach, based on a strong integration between Information & Cyber and Physical & Corporate Security.

The adoption of a holistic approach for Security leads to the integration of processes and tools for the identification, evaluation and management of security risks and to an effective security convergence where Information & Cyber and Physical & Corporate Security objectives are strictly aligned. This integrated security approach brings together the various functions and dependencies with other parts of the organization, enabling the resilience of the Group to incidents.

The Security strategy defines a path to achieve the Security mission of Generali Group, leveraging on the following main drivers:

- **Incident prevention and protection from security threats**: the level of exposure to security risks - in particular referring to cyber security risks - are constantly monitored to implement and improve adequate security measures that guarantee the protection of company assets in terms of people, information and physical assets;
- **Management of security risks with specific focus on third-party providers**: the level of exposure to security risks and especially the risk related to data managed by third parties requires constant assessment of their behavior, performance and security frameworks on which the relationship is based;
- **Business alignment**: new innovative and digital services require adequate security levels and resilience;
- **Regulatory compliance**: external demands in terms of compliance and regulation require meeting specific regulatory demands, including personal data protection and security.

To properly and effectively apply the above principles, Generali Group has adopted a security management process based on the following sub-processes: identification, protection, detection, response and recovery. These sub-processes are performed concurrently and continuously to form an operational culture that addresses the Group Security.