Generali Group

SECURITY GROUP POLICY

Group Chief Security Officer

GROUP POLICY

Public version

generali.com

General Principles

The Generali Group has an important capital in terms of physical and information assets, as well as cultural heritage (hereinafter Company Asset), that needs to be protected especially from Security Incidents and Threats.

In this context, the Generali Group defines a **Security Strategy** and a corresponding **Security Strategic Plan** to be shared and implemented across the Group leveraging on:

- a **system of governance** centred around the key roles of the Group/BU/Local Security Officers and with clearly defined responsibilities for all involved functions at GHO, BU and Local level;
- a **common process** to manage all security aspects and issues at GHO, BU and Local level;
- a **common model** to manage critical events and business continuity across the

The above principles commonly apply to all following security areas (*One security approach)*:

- **IT Security**: protection of infrastructure, application, endpoints, mobiles and data;
- **Cyber Security:** prevention of and response to security incidents and system vulnerabilities;
- **Physical Security**: protection of company buildings and internal workspaces, as well as employees during business travels[1];
- **Corporate Security:** management of security aspects in most relevant corporate Events (e.g. Shareholders' meeting, GLG' meeting etc.), business intelligence activities on digital media and malicious activities on the web, even in collaboration with the relevant public authorities.

The provisions of this Group Policy and the relevant implementing Group internal regulations are defined according to the Digital Operational Resilience Strategy (DORS) from time to time approved by the AG BoD.

[1] Safe of personnel on workplaces is out of the scope of this Group internal regulation and it is described in other specific documents.