Abstract of Security Policy

CONTENTS

1 FOREWORD

The primary responsibility of Banca Generali, within the competitive environment and financial sector in which it operates, is to protect the tangible and intangible assets at its disposal from any attack and unauthorised access.

This Security Policy (hereinafter also referred to as “Policy”) describes the objectives, principles and main security-related responsibilities within Banca Generali and covers:

- ***IT Security****,* which concerns the protection of data and information systems from unauthorised access, use, disclosure, blocking, modification or deletion in order to provide confidentiality, integrity and availability of data;
- ***Cyber Security***, which includes the ability to prevent security incidents or vulnerabilities of information systems and protect/defend the use of Internet networks against cyber attacks;
- ***Physical Security****,* which aims to ensure protection from unauthorised access to premises, equipment and resources, and the protection of Personnel during business trips and travels;
- ***Corporate Security****,* which, on the one hand, concerns the management of security aspects in the main corporate events (e.g., the General Shareholders’ Meeting) and, on the other hand, brand abuse, social intelligence and business intelligence activities, including to protect intellectual property from attacks and damage (e.g., industrial espionage and data theft), also carried out in collaboration with external bodies, as well as national and local public authorities in order to collect information relating to specific cyber and physical threats related to the monitored brands.

The Policy is based on international standards, frameworks and best practices and complements the regulatory corpus of policies that the Bank has adopted to define the principles and guidelines for the security of IT applications and integrated management of information data, in order to support the Bank in adopting data-driven decisions and strategies. Occupational health and safety issues pursuant to Legislative Decree No. 81 of 9 April 2008 do not fall within the scope of this Policy.
The principles and requirements relating to IT Security are laid out in greater detail in the Bank's second-level policies.

2 SCOPE OF APPLICATION

This Policy applies to all employees and collaborators of Banca Generali and of the Banking Group companies.

2.1 Roles and Responsibilities

In its capacity as the strategic oversight body, the **Board of Directors** is promptly informed in the event of any critical incidents or significant security-related events. Moreover, the Board of Directors:

- approves the strategies for the development of the IT system and its architecture, in light of the outsourcing guidelines adopted and in keeping with the current and future structure of the Company's sectors of operation, processes and organisation;
- is informed promptly by the Chief Executive Officer and/or the Corporate Control Functions involved in the event of severe problems for company activity arising from incidents and malfunctions affecting the IT system;
- approves the IT risk appetite, with regard to internal services and those offered to customers, in accordance with the risk targets set in the RAF (Risk Appetite Framework);
- ensures that the governance system — and, where applicable, the risk management and internal control system — adequately manage security risk, within the broader framework of operating risks;
- guarantees the adoption and implementation of the security strategy and security governance model of Banca Generali, in line with the Generali Group’s policies;
- ensures the implementation of Banca Generali's security strategic plan, in line with the Generali Group’s policies.

As the body with managing functions, the **Chief Executive Officer/General Manager**:

- upon proposal by of the COO, appoints the Chief Security Officer;
- defines security measures, based on the recommendations of the Chief Security Officer;
- annually approves the Operational Security Plan and the Report on the implementation progress of security initiatives;
- takes timely decisions in the event of serious security incidents or significant malfunctions;
- approves, generally with annual frequency, the operational plan for IT initiatives, verifying that they are consistent with the IT and automation requirements of the business lines and company strategies;

- takes timely decisions regarding serious IT security incidents and, with the support of Corporate Control Functions, provides information to the Board of Directors in the event of severe problems with company activity arising from incidents and malfunctions.

The **Risk Committee** supports the Chief Executive Officer in the supervision of implementing activities and the development of the Bank's security strategy.

Within the framework of the Risk Committee's activities, security-related issues are discussed on a half-yearly basis for a holistic examination of the various components to ensure an integrated vision of the various specialist domains and areas of competence, by the Chief Security Officer, in the presence of the Head of the COO & Innovation Area, the Head of the Alternative and Support Channels Area, the Head of the Human Resources Department and the Head of the Marketing and External Relations Department.

The **Internal Audit Department**, as part of its control tasks, periodically verifies the effectiveness and efficacy of standards, controls, policies and procedures defined and, on an annual basis, submits to the Board of Directors a specific security assessment report.

The main responsibility of the **Chief Security Officer** (CSO) is defining the Bank's security strategic vision, implementing programmes to protect information assets and guaranteeing IT infrastructures security, as well as identifying, developing and implementing processes aimed at mitigating the risks arising from the adoption of digital technologies.
The Chief Security Officer is therefore responsible for:

- developing the security strategy and governance;
- coordinating the security-related issues, with the support of the organisational structures involved in the different processes;
- managing corporate security aspects, in concert with the Risk Management function and in accordance with the reputational risk management methodological framework, while supporting, within this area, the structure tasked with managing the most relevant corporate events;
- managing IT security and cyber security aspects, in concert with the Risk Management function and in accordance with the operational risk management methodological framework, which also include IT risks;

- implementing the Bank's Security Plan, in accordance and consistent with the Insurance Group's Strategic Security Plan. In order to ensure proper implementation of the Security Plan, the Chief Security Officer assesses the specific Bank's requirements in terms of budget, investment planning and resources (including, among others, financial, human and technological resources);
- identifying risks for security by ensuring the appropriate mitigation measures, while also promoting a security culture through training and awareness-raising programmes;
- monitoring and preventing digital and Web brand abuse activities;
- checking compliance with IT security requirements of all major changes to IT systems and services;
- informing the COO and the Chief Executive Officer on the implementation of the Operational Security Plan, the related necessary resources, and the security threats or critical incidents that occurred in the reference period;
- promoting and convening, as a rule every six months, a roundtable discussion with the structures responsible for the relevant areas for a holistic examination of the various components; the discussion is attended by the COO, who coordinates the roundtable, the internal Head of Facility Management, the Chief Security Officer and the Head of Human Resources, as well as the Head of Marketing and External Relations;
- managing the activities aimed at updating the Banking Group's Business Continuity Plan (BCP) and implementing the identified continuity solutions;
- ensuring all security measures aimed at guaranteeing personal data protection, collaborating in this regard with the Data Protection Officer;
- ensuring, with the support of the Internal Rules Service, the updating of this Policy.

The Chief Security Officer must be endowed with resources adequate to his or her responsibilities, must not be involved in business activities in order to avoid conflicts of interest and must report directly to the Head of the COO & Innovation Area.

The Head of the **COO & Innovation Area** is responsible for:

- supervising the implementation of the Bank's Security Plan and security initiatives;
- supervising the adequate implementation of Security Measures and periodically informing the Risk Committee of the security strategy for the areas within his or her remit, the formulation and implementation of the Operational Security Plan and security threats or critical incidents that have occurred during the period of reference;
- approving and submitting, through the Chief Executive Officer, guidelines, directives and standards for IT Security management to the attention of the Board of Directors with regard to the evolution of the field of activity, products offered and technologies;
- assuming the highest level of responsibility in managing highly critical situations, supporting the preparation of any communications for Supervisory Authorities and/or the corresponding role at Group level.

In line with Banca Generali's HR processes and legislative requirements, the Security Governance Model is structured as follows:

- Sourcing: the hiring and termination of the CSO are the responsibility of the Head of the COO & Innovation Area (in consultation with the Human Resources Department), in concert with the Chief Executive Officer/General Manager.

- Performance measurement: the formulation of the objectives and assessment of the CSO's objectives are the responsibility of the Head of the COO & Innovation Area in concert with the Chief Executive Officer/General Manager, according to the Group's procedures and processes in effect from time to time.

The Head of the **Alternative and Support Channels Area** is responsible for:

- implementing operational aspects relating to Physical Security in coordination with the Chief Security Officer on the basis of the Security Plan;
- managing the Insurance Group's facility management outsourcers, with regard to the issues under his or her remit;
- on the basis of the Physical Security risks identified by the Chief Security Officer, ensuring the appropriate mitigation measures;
- verifying the compliance with Physical Security requirements of all substantial modifications to the Bank's offices, branches and premises;
- promptly informing the Chief Security Officer of security threats or critical incidents (e.g., robberies) that have occurred;
- with regard to Physical Security incidents, supporting the Chief Security Officer in preparing the relevant section of the information report.

In the area of personnel security (e.g., robberies), the Alternative and Support Channels Area receives support and collaboration from the Human Resources Department.

With regard to Physical Security, the **Human Resources Department** is responsible, in coordination with the Chief Security Officer, for the operational aspects of personnel security regarding business travel and trips.

With regard to Corporate Security, the **Marketing and External Relations Department**, in coordination with the Chief Security Officer, is responsible for aspects of operational security relating to the organisation of company events.

3 SECURITY MISSION AND STRATEGY

The Bank's mission is to protect all the Company’s physical and IT resources and cultural assets, defining a common approach for managing security elements and promoting a culture of security within the Group.

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

The adoption of a holistic approach is instrumental to the integration of processes, procedures and tools for the identification, evaluation and management of security risks and to an effective security convergence, where IT Security, Cyber Security, Physical Security and Corporate Security objectives overlap and are strictly aligned. This integrated security approach brings together the Bank’s various structures dealing with security in their various capacities and other parts of the organisation, enabling the Bank’s resilience to incidents.

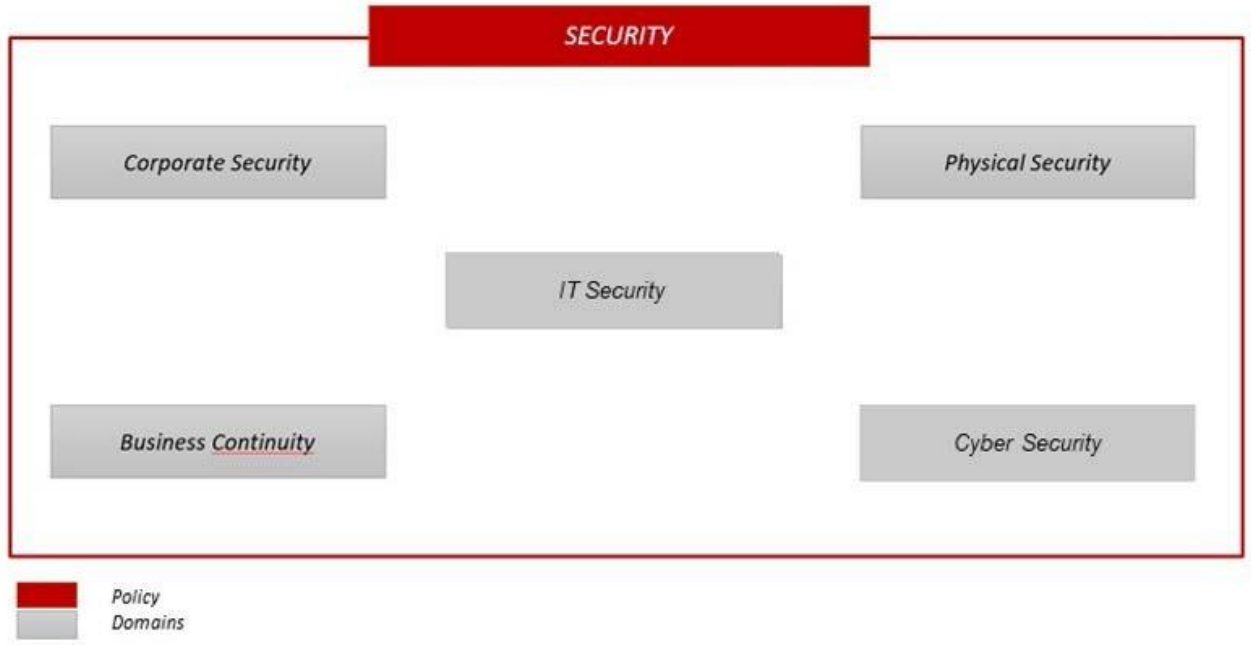
The security strategy defines a path to achieve the security mission for company assets, in line with the Group’s mission, leveraging the following main drivers:

- *Incident prevention and protection from security threats*: the level of exposure to security risks — in particular with reference to cyber security risks — is to be constantly monitored to implement and improve adequate security measures that guarantee the protection of company resources 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 the behaviour of such parties, their performance and the 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.

4 SECURITY GOVERNANCE

4.1 Security Domains

This Policy includes the following security domains, as described below.



IT Security is a primary aspect for ensuring the continuity of the Bank's activities and protecting the data of customers, employees and business partners, and concerns the protection of infrastructure, application, endpoints, mobile devices and data.

Cyber Security refers to the prevention, identification and response to security incidents and system vulnerabilities and the protection of data and information throughout the life cycle from unauthorised access, use, disclosure, destruction, modification or interruption, also taking into account the growing relevance of cyber threats globally.

Corporate Security aims to preserve assets and intellectual property and includes principles and requirements designed to prevent, deter, delay and mitigate possible threats, minimise related consequences and manage security aspects in an adequate and timely

manner in the most relevant corporate events (e.g., the General Shareholders' Meeting). It also concerns business intelligence activities carried out in collaboration with local and national public authorities in order to collect information relating to specific economic, political and financial situations related to countries and/or competitors and partners. Corporate Security also refers to security intelligence activities for the protection of the Bank's brands and products, monitoring communications on digital media and malicious activities on the Web.

Physical Security includes principles and requirements designed to prevent, deter, delay and mitigate possible threats, minimise related consequences and manage potential security incidents related to workplaces and personnel in an adequate and timely manner. Physical Security refers to the definition, implementation and monitoring of the physical security measures necessary to ensure a minimum level of security of company buildings and internal workspaces, adopting a risk-based approach. It includes the definition and implementation of actions and measures to be taken in order to ensure the security of Personnel during business trips.

Business Continuity refers to the identification of an organisation's priorities and preparation of solutions to address disruptive threats, providing a framework for an effective response that safeguards the interests of its key stakeholders, reputation, and value creation activities. The business continuity domain includes identifying critical operations and risks, preparing plans to maintain or restore critical operations during a crisis, and creating plans to communicate with key people in the course of such events.

4.2 Security Management Process

In order to correctly and effectively apply the above-mentioned principles, the Bank has adopted a security management process based on the following sub-processes:

A) identification,

B) protection,

C) detection,

D) response,

E) recovery.

These sub-processes should be performed continuously to form an operational culture that addresses the Bank’s security.

- *Identification*

At the beginning of the process, the security risk must be identified taking into account the Company Resources and relevant regulatory requirements, defining the exposure to the security risk.

The Chief Security Officer is in charge of identifying security risks, as well as all the Security Measures and specific needs of the Bank necessary to mitigate them, and receives support from and collaborates with the Bank's other structures that oversee particular operational security areas.

The Chief Security Officer must take into account:

- the security risks relating to the Bank's operations (IT processes and systems), company assets and personnel;
- security rules based on external supervisory provisions and the internal corpus of security regulations, and the specific activities performed to manage and monitor the Bank's compliance with security requirements;
- the company context based on the Bank's mission and strategy, its objectives, the type of business industry, its stakeholders and main activities;
- management of company assets based on data, personnel, IT devices, IT systems and infrastructure that allow the Bank to implement its security strategy and ensure the management of security aspects;
- third-party security management, based on all security risks associated with such third parties.

Therefore, the CSO is responsible for implementing — in close collaboration with the Risk Management function and with the support, where necessary, of the IT & Operations Department — the IT & Cyber Security risk management methods and the related assessment activities, as well as periodically discussing and aligning with the Risk Management function so as to review the Bank's security risks.

- *Protection*

This process makes it possible to define the security measures to be implemented in order to protect the Bank's resources during the execution of business procedures based on the risks and actions identified in the previous phase. In addition, it is also necessary to evaluate the actions to be taken to ensure the correct implementation of the Operational Security Plan of the Bank and the Banking Group. Security measures refer to the following areas:

- User management and access and authentication control: limiting (physical and logical) access to Company Resources to authorised users, processes and devices;
- Staff awareness and training on security areas;
- Data security: ensuring adequate protection of information classified, archived or transmitted, whether onsite or offsite;
- Information protection processes and procedures;
- Maintenance and restoration of the functionalities and performance of company assets;
- Technologies and protection systems aimed at ensuring the security and resilience of IT systems: ensuring the use of adequate technical solutions, the protection and resilience of Company Resources, and in particular of IT systems.

Staff awareness and education on security areas

Awareness-raising and education measures are designed to raise awareness among the Bank's personnel of the importance of adequately protecting and processing sensitive information, preventing, intercepting and reporting events or behaviours that may cause damage to the Bank.

In light of the tools available internally and provided at the Group level, the education plans formulated by the Human Resources Department or other methods deemed appropriate from time to time, the following activities must be planned regularly:

- formulation of the type of initiatives to take, the target participants and/or beneficiaries of reference and methods of execution (e.g., e-mail campaign, classroom sessions, technical courses, etc.);
- preparation, where not already available, of the material needed to execute the initiative identified;

- organisation of awareness-raising and education events, including the preparation of an annual education plan for all employees and, for personnel tasked with critical functions (critical or important functions), preparation of an ad-hoc annual education plan on Information Security;
- participation of all Bank personnel in education, awareness-raising and refresher courses on IT security.

- *Detection*

This process identifies the occurrence of a security event, through early detection of unusual activity and continuous monitoring of potential threats and assessment of potential impacts. At this stage, the Chief Security Officer is in charge of putting in place the appropriate activities for the timely detection of any security incident that could affect the Company Resources.

To this end, the Chief Security Officer is responsible for coordinating the continuous monitoring of potential threats from the external environment or third parties and the assessment of potential impacts. Should a Security Incident occur, the Chief Security Officer must promptly take the initial actions needed

- *Response*

Following the detection of a security event, this process defines appropriate activities to be carried out in order to activate response procedures and mitigation activities with timely execution. Learning from detection/response activities is part of this process.

In the event of a Severe Incident, the CSO must promptly launch crisis management processes and inform the Head of the COO & Innovation Area and the Chief Executive Officer, who will approve the relevant solutions. If necessary, the pertinent business continuity measures envisaged in the Business Continuity Plan must also be taken into consideration.

- *Recovery*

This process allows appropriate activities to be developed and implemented in order to maintain resilience plans and restore all capabilities or services affected by a security event, ensuring a timely recovery of the information systems and/or physical resources affected.

to manage it, activating the appropriate incident response team (IRT).

4.3 Operational Security Plan and Annual Report on the Implementation Progress of Security Initiatives

The Operational Security Plan is defined by the COO & Innovation Area, through the Chief Security Officer and with the support of the structures involved, each within its remit, and submitted — as part of a joint document — to the Risk Committee for an opinion in order to prepare a summary version including the key elements. The Plan is then submitted to the Chief Executive Officer for approval.

The Chief Security Officer prepares an Annual Report on the Implementation Progress of Security Initiatives on critical incidents occurred and education initiatives taken. In order to ensure an integrated vision of the various areas of security, the Chief Security Officer will have the support of the structures involved in the operational aspects of security.

The Chief Executive Officer submits the Report, together with the Operational Security Plan, to the attention of the Board of Directors.

4.4 Annual IT Security Assessment Report

As part of its responsibilities, the Internal Audit Department prepares, within the first half of the year following the year of the analysis, the Annual IT Security Assessment Report focused on the IT system governance and organisation, IT application and information security, control measures, etc.

4.5 Information Security Measuring and Reporting Performance

The purpose of this area is to permit the Bank to assess over time the efficacy of its Security Management Model on the basis of the information made available by suppliers and internal resources, including through the use of appropriate key performance indicators (KPIs). The aim is thus to facilitate the identification of improvement measures and the strengthening of its own processes, procedures, services, activities and support technologies and tools.

The identification and collection of the KPIs is responsibility of the Security and BCP Service.

Moreover, on a quarterly basis, the Security and BCP Service shares, with the Risk Management Department, the Cyber Risk KPI, which is integrated within the RAF.