*In case of inconsistency or conflict between versions of the document, the Italian version shall prevail over any translation*


# General security principles

## GENERAL PRINCIPLES

The rapid evolution of information systems, related procedures and global threats requires a growing focus on risks threatening information assets, provided services and, therefore, people including their assets and their privacy rights.

FinecoBank Group places a high value on the security of information and its information systems and considers these as:

- a strategic asset to develop and manage our business;
- a key success factor for business development and strengthening our Group reputation;
- an outstanding element to provide high quality and reliable services as well as thorough data management.

From this perspective, **information security is considered a key-driver to assure customer and stakeholder interests, resiliency of business critical systems as well as compliance with regulations**: in this context, the Group addresses and manages information security in accordance with major international standards, frameworks and best practices.

These aspects require implementations are aligned with the **Group Security Management System**, including internal regulations, policies, procedures, manuals, both organisational and technical measures, as well as **a structured organisational model aimed to ensure the continuous improvement of the implemented measures** to face **evolving threats**, both external and internal.

Therefore, information security governance and management processes, activities and related risks are structured involving Bank corporate bodies and functions, in accordance with their respective responsibilities and with the *three lines of defence model* implemented through the Internal Control System.

The outcome of the described approach sets out an information security framework which establishes periodical evaluation, review and enhancement activities that ensure:

- security governance and alignment with **Group Business and ICT & Security strategy**;
- a shared, documented, organic, efficient and effective **security organisation**;
- **continuous monitoring** of the security threat landscape;
- coordination and optimisation of available **resources**;
- implementation of both **preventive and reactive security measures** according to a multi-level security model consistent with the “defence **in depth**” principle;
- integration of security procedures within corporate processes, in order to ensure that both identification and management of security risks are part of Bank initiatives as a security by design and default element;
- **skills** and **awareness** development **on information & cyber security risks and threats**, through continuous training and awareness-raising activities;

- **active monitoring of system and security events**, as well as **technical vulnerabilities** management, through **threat intelligence, vulnerability assessment and penetration testing campaigns**, in order to prevent and identify cyber threats against the Group;
- **security event management** through a structured **incident and crisis management** process;
- **compliance with** relevant **regulations**;
- **third-party and outsourced-activity security** through appropriate contractual agreements and ongoing monitoring during the whole contract terms.