INFORMATION ON

PHYSICAL SAFETY

Grupo Santander

CONTENT

This document sets out the Physical Safety Policy, which establishes principles and functional aspects for protecting the physical integrity of the Group's essential assets (i.e. customers, employees, facilities and information).

It also sets out principles for coordinated action regarding physical safety in the Group, with value add and guidance for the various units that will raise service quality.

It draws from the general frameworks for risks, compliance and conduct, cybersecurity, special situations management and intelligence services and from the procedure for reporting and escalating significant operational risk events within the Group.

1 POLICY GOVERNANCE

Physical safety management consists of prevention, detection and response processes and mechanisms to protect customers, employees, facilities and information from security incidents relating to material damage and fraud according to the Basel Committee's classification of operational risk. It also involves cooperation in crisis situations resulting from natural disasters or other events that may affect business operations.

This policy contains the following definitions:

- **Physical safety**: Rules, systems and processes for protecting the physical integrity of things found in a given space.
- **Personal safety**: Physical safety rules, systems and procedures for safeguarding the bodily integrity of employees, customers, shareholders, guests and visitors (including temporary or occasional consultants and auditors) in a given space.
- **Building safety**: Materials, electronics and personnel for protecting the surroundings and the interior of buildings, including employees, customers and visitors inside them.
- **Critical infrastructure:** Strategic infrastructure that is essential to basic services and cannot be substituted if tampered with or destroyed.
- **Basic service:** An essential service that cannot be substituted and would have serious consequences if tampered with.
- **Essential assets**: Customers, employees, facilities, IT platforms and information (data).

This Policy does not cover actions logically intended to safeguard information, which are described by the rules set out in the Cybersecurity framework.

2 PRINCIPLES

Physical safety action must adhere to and uphold the following principles

2.1 Physical safety duties

Because of both the function's special nature and correct physical safety management, duties must be clearly defined to design, approve, implement, monitor and revise security plans and ensure that the corporation and subsidiaries coordinate properly.

The Security and intelligence function will be led by a corporate security director at the Corporation. Per the Group's instructions, the subsidiary security and intelligence function must report to a security director.

If a unit cannot have a security director because of its size, it must designate someone who will guarantee the utmost confidentiality the role requires in order to liaise with the corporate function.

Nonetheless, every employee is in charge of keeping themselves and any assets assigned to them safe and should follow the safety guidelines, ethical principles and rules set out in the Code of conduct.

2.2 Risk analysis and asset classification

Techniques for assessing risks and weaknesses should be used to classify assets by level of importance and establish mitigating measures.

Assets will be reviewed and classified by level of importance in order to establish security measures that prioritize protecting the most critical assets.

2.3 Adequate resources

The Security and intelligence function should make sure resources are assigned to make (and keep) people and assets safe. It also must establish the specific processes for the security and intelligence functions to follow, based on efficiency, effectiveness and cost rationalization to optimize protection and achieve the highest possible level of security.

The human resources assigned to the function must possess the knowledge and credentials required for their role.

2.4 Safety of people and assets

To ensure the safety of people and buildings, all important buildings, critical facilities and institutional events will have proper protection plans in place.

Data Processing Centres (DPCs) and other areas deemed "restricted" will be subject to special access control and supervision protocol.

2.5 Forward-looking analysis and intelligence

To enhance security management in a forward-looking and preventative manner, the Security and intelligence function must establish review processes to examine current situations, anticipate outcomes and set standards to ensure the right level of protection for customers, employees, facilities and information.

Intelligence and analysis procedures are systematic and logical and aim to collect, review and manage information, improve security planning and decision-making, and protect the business, assets and people.

2.6 Coordination with the Corporation

Security and intelligence directors at the Corporation and the subsidiaries will properly coordinate the function to ensure first-rate security management, share best practice and add value.

They must have procedures and rules for escalating major security incidents in order to be able to perform coordination and support duties, cover regulatory needs and ensure that such procedures and

rules are adequately aligned with the procedure for reporting and escalating significant operational risk events.

Reporting will be based on level of importance and frequency.

2.7 Business safety

The Security and intelligence function is in charge of ensuring and safeguarding essential assets for business operations (branch networks, points of sale, ATMs, centres of operations and shared services) and implementing proper protection plans for all aspects of the business.

2.8 Fast and effective response to “special” situations

The Security and intelligence function must establish measures, rules and guidelines to respond quickly and effectively to emergencies that could damage the Group's physical and/or human resources or hinder normal business operations, in accordance with the Framework for Special Situations Management and the manner set out under the Special Situations Management Model.

2.9 Physical safety of information

The Security and intelligence function must ensure that information is physically protected and subject to controls based on the data it contains.

2.10 Cooperation with law enforcement

Someone must be designated to liaise with police agencies if working and coordinating with law enforcement institutions and agencies becomes necessary due to inquiries into classified events or damage caused to physical assets and/or internal/external fraud. For international or supranational incidents, the corporate Security and intelligence function will be in charge of liaising with law enforcement agencies on behalf of all the entities within the Group.

2.11 Oversight of contractors

The Security and intelligence function will oversee contractors that perform security activities, especially ones deemed most critical and which have been outsourced.
It will act as a special function and set standards for authorizing third parties according to physical safety risks.

2.12 Insider threats

The corporate Security and intelligence function will be in charge of coordinating the programme for preventing and detecting insider threats to the Group, alongside other special functions.

2.13 Safety of travelling and expatriated employees

The Security and intelligence function will make sure all employees who are travelling internationally or expatriated receive training and information about risks to their security and health and necessary protection and prevention measures during their sojourn.

It is also in charge, therefore, of the global programme for protecting travellers, in which it will provide travelling and/or expatriated employees with protection and advice during and after their travels.

2.14 Training

To ensure effective security, all employees must undergo training courses and have guides, which must come with awareness campaigns.

The Security and intelligence function must also make sure security staff and human resources tasked with safety are properly trained.

The Group's entities will draw up rules and plans for training to ensure proper security instruction for employees and human resources tasked with safety. Therefore, the Governance and subsidiary coordination function will create manuals and guides on good practices.

3 POLICY GOVERNANCE

The Physical safety policy is approved by the General Secretary of Banco Santander, S.A. as division head. It will be regularly revised as part of a constant improvement process. To be effectively implemented, it will be distributed to subsidiaries of Grupo Santander as a reference document.