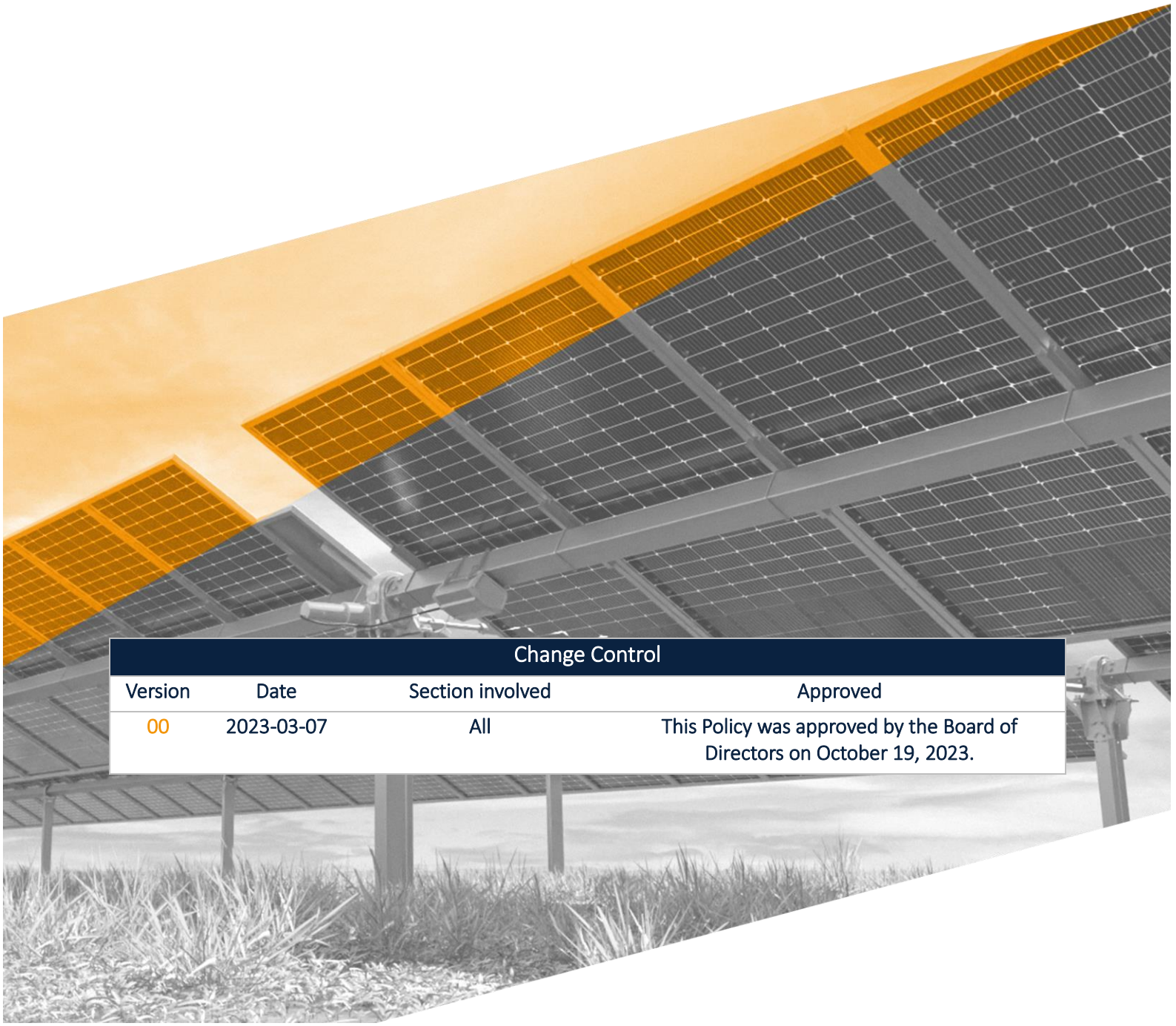
Physical, Property and Corporate Security Policy

CP-SE-0001_en



Change Control			
Version	Date	Section involved	Approved
00	2023-03-07	All	This Policy was approved by the Board of Directors on October 19, 2023.

Content

1 Introduction 3
2 Purpose 3
3 Scope of Application 3
4 Roles of the Corporate Security Department 3
5 Basic Principles of Corporate Security Department Action 4
6 Collaboration and Suggestions Through Corporate Mail 5
7 Penalty Regime 5

1 Introduction

Soltec Power Holdings, S.A. (hereinafter the "Corporation" or "Soltec") and the companies within its group (hereinafter ''Group'') operates worldwide. In accordance with Article 249 bis of Spain's Capital Companies Act, SOLTEC's Board of Directors has the responsibility of determining the general policies applicable to the entire Group.
The Capital Companies Act also establishes that the Board of Directors is responsible for defining the Holding's general comprehensive security strategy.

2 Purpose

The purpose of this policy is to lay down the basic principles and guidelines governing the Group's physical and property security strategy, as well as to guarantee the effective protection of people, physical and logical assets, infrastructures, projects and information. This should be achieved with a reasonable, optimum level of security, resilience and compliance to fulfill the functions required by current legislation, while integrating this policy with other corporate policies implemented by Soltec to date.

3 Scope of Application

This Policy applies to all Group companies and all their employees, in all Group sites, as well as to any other stakeholder.
As a requirement to enter into any type of business relationship with the Group, any third party seeking to contract with the Group must expressly sign its acceptance of this Policy and the obligations deriving from it, in particular the Group's zero tolerance for the commission of criminal acts, both by Group members and by third parties with whom the Group enters into a contract. In this sense, the Group reserves the right to require from business partners with whom it establishes relationships, a general compliance management system or equivalent measure with the aim to ensure compliance with the above-mentioned; it may also terminate any contractual relationship in case of non-compliance with the foregoing on the part of any third party.

4 Roles of the Corporate Security Department

The Corporate Security Department is responsible within the Group for the supervision, surveillance and control of obligations arising from the regulations governing private security. The Corporate Security Department, which shall meet such responsibility for the entire Group at a corporate level, will perform the following functions, among others:

- To identify vulnerabilities through situational analysis of activities and regions.
- To communicate and respond to incidents related to Physical, Property and Corporate Security.
- To conduct and coordinate investigations and analyses derived from criminal activities and to identify opportunities for reducing potential threats with in-house processes.

- To maintain close cross-functional cooperation with all Group departments, as well as with collaborators, customers, suppliers and contractors.
- To establish expectations for each asset, procedure and management indicator, preparing, supervising and auditing company facilities to ensure consistent implementation of programs and measures for prevention and protection (security).
- To manage resources needed for surveillance, access control, prevention mechanisms, deterrence and monitoring within the professional environment.
- To maintain ongoing contact with authorities and other stakeholders with the aim of actively anticipating scenarios or situations of vulnerability or potentially threatening.
- In case of events requiring the activation of response mechanisms, to act with the intent of minimizing losses and with an approach that favors improved response times, as well as to share timely information facilitating the organization's decision-making process.

Corporate Security Department actions should be developed within a framework of ethics and responsibility, in compliance with current legislation and applicable regulations at all times, as well as in accordance with in-house protocols and procedures.
For an **effective application** of this policy, it is necessary to ensure the participation of all Group employees and of active or necessary collaborators, so that based on the premise “Security is everyone's business”, the policy can be rolled out supported by collaboration between all Group departments and employees.

5 Basic Principles of Corporate Security Department Action

To achieve this commitment, the Group assumes and promotes the following basic principles of action which must govern all Group activities in the area of physical, property and corporate security. This principle, channeled through the Corporate Security Department, aims to coordinate and implement measures for the prevention and detection of situations threatening the normal course of activities or the company's image, while increasing operational reliability and providing peace of mind to personnel in the development of their work.

The following actions should be implemented within the development of this Policy:

a. To design a comprehensive preventive security strategy aimed at minimizing physical, property and logistical security risks, including the consequences resulting from a terrorist threat or act, and to allocate the necessary resources to implement such strategy.
b. To develop specific defense plans for the protection of infrastructures/projects and to guarantee the continuity of essential services provided by Group companies in case of emergency or crisis.
c. To guarantee the protection of professionals in the Group companies, both in their usual workplace and when traveling for work-related reasons (*duty of care*).
d. To ensure adequate protection of data and of the Group's control, information and communication systems, in accordance with the provisions of the information security management section and other protocols that may be developed in this regard.
e. To have procedures and tools in place to actively combat crime and attacks on the brand

and on the reputation of the Group and its professionals.

f. To adhere to current legal regulations and to adapt operating procedures to their guidelines, acting at all times in compliance with applicable legislation and within the framework of other Soltec in-house rules.
g. To implement and develop corporate security measures based on criteria of efficiency and effectiveness, with the aim of reinforcing existing security and of contributing to the normal development of the Group's activities.
h. To avoid the use of force in the exercise of security actions, using it only and exclusively when it is strictly necessary, always in accordance with the law and in a level proportional to the threat received, complying and adapting the action to applicable national and international regulatory norms.
i. To promote a culture and awareness of security within the Group by carrying out dissemination and training activities in this area.
j. To ensure the adequate qualification of all corporate security personnel, both internal and external, by establishing rigorous training plans and defining recruitment requirements and criteria which take this principle into account. In particular, to train all security personnel in human rights or to ensure they have received adequate training in this area. To transfer these principles to contracted security providers and to periodically evaluate their compliance and monitor their suitability to perform their functions for the Soltec Group.
k. To collaborate with authorities and agencies responsible for security matters and not to interfere in the fulfillment of their legitimate functions, being their liaison and point of contact in aspects relating to public security, private security and other forms of protective security within the industry.

6 Collaboration and Suggestions Through Corporate Mail

In order to collaborate, suggest or report any irregularity detected or non-compliance with these policies, or simply to clarify any doubts, a suggestion box managed by Soltec's Security Department was set up and made available to employees, whose anonymity is maintained:

security@soltec.com

7 Penalty Regime

Non-compliance with the physical, property and corporate security policy: Penalty regime.
In case of non-compliance by any employee or collaborator with the Group's security policy, the penalty regime established in the Workers' Statute and in the Collective Bargaining Agreement signed by the company shall apply. The penalty regime should be commensurate to the seriousness of the conduct (except in case of an infringement which constitutes a criminal act and must therefore be sanctioned and prosecuted accordingly. Such infringement will be immediately brought to the attention of the authorities).
The Group's Human Resources Department will be in charge of adapting the corresponding penalty to each conduct on an individual basis.

This Policy was approved by the Board of Directors on October 19, 2023.