DATA SECURITY POLICY

Solaria

Contents

INTRODUCTION

At Solaria Energía y Medio Ambiente, S.A. (hereinafter, "Solaria" or the "Company"), we believe that the information we handle is one of our most important resources. It is therefore a duty and an obligation to take security measures and to apply suitable operating processes that ensure the correct functioning of the Company and protection of information in order to create a secure environment for employees, collaborators, suppliers, customers, shareholders, investors and all other third parties with whom the Company interacts.

The purpose of this data security policy (hereinafter, the "Policy") is to create effective protection of the aforementioned information. Specifically, it seeks to guarantee the confidentiality, integrity and availability of Solaria's information; compliance with applicable legislation; balance between levels of risk and efficient use of resources and continuity of the business.

The information handled by the Company may appear in different kinds of media: in written or printed form, stored electronically, transmitted by post or by electronic media, shown as projections or heard in conversations. Regardless of the format that contains the information, it is necessary to establish a system that manages the security of the information to protect it from threats.

In this sense, data security is defined as the safeguarding and protection of (i) data owned by Solaria, whether they are in Solaria's systems or those of third parties, and (ii) data owned by third parties that are in Solaria's systems.

Data protection is among Solaria's corporate policies, which are designed to manage risk and minimize corporate breaches of law.

Solaria

PURPOSE

The purpose of the Policy is to establish the framework of action needed to protect the data resources from internal or external threats, both accidental and deliberate, in order to ensure the confidentiality, integrity and availability of the information.

Data security involves the access, use, disclosure, interruption and unauthorized destruction of information. The security system is based on minimization of risk and targets the adoption of a series of procedures to improve data security.

More specifically, the Policy has the following objectives:

- Understand and deal with operational and strategic risks in relation to the security of Solaria's information as a means of keeping it at acceptable levels.

- Protect the confidentiality of the information.

- Understand and meet the needs of all parties involved.

SCOPE

This Policy applies to Solaria and its group companies (hereinafter "Solaria Group") and affects all of their employees, regardless of position and function.

The Policy may also be applied partially or fully to any other individuals or legal entities that are associated with Solaria Group for reasons other than professional relations when it is possible to do so due to the nature of the relation and it is of intrest to the parties for the purpose of fulfilling said relation.

BASIC COMMITMENTS

Solaria understands the importance of proper handling of information and has set forth this policy of commitment to the implementation, operation and ongoing improvement

of the data security management system in an effort to establish a framework of confidence for all interested parties that maintain any type of relation with Solaria.

The principles of data security, according to Solaria, are the following:

- Confidentiality: The information must be known only by authorized persons.

- Integrity: The information must be complete, precise, valid and not subject to manipulation.

- Availability: The information must be accessible to authorized users at all times and its persistence in any unforeseen event must be guaranteed.

MANAGEMENT OF DATA SECURITY

After detecting the main risks that pose a threat, the Company takes the following measures to protect the data it processes and to minimize said risks:

- Use of systems: The use of systems and computers is limited to legal and professional purposes in the completion of job-related tasks. Therefore, systems and computers must not be used for any illegal purpose.

  Employees must make sure that the Company's computers are handled, used and maintained properly.

- Controlled access: Solaria has established a system of password-protected user access to any digitized information. In addition, the Company has defined roles and permits for its employees on the basis of their positions and their needs so that they may access certain types of information within the system.

- Cryptography: Solaria has established a system in which accessed data must be uploaded to the cloud and encrypted. It is not allowed to store information on employees' local drives without password-protected access.

- Protection of installations, systems and environment.

- Default security.

- Integrity and updating of system.

- Protection of stored information and data in transit.

- Classification of information: The documented information is classified as public, internal or confidential and is used in accordance with the assigned classification.

COMPLIANCE

The Board of Directors of Solaria, through the Ethics, Compliance and ESG Commission, is in charge of approving this Policy and of supervising and periodically evaluating its implementation.

Internally, the systems controller is in charge of monitoring and verifying compliance with this policy and of proposing any necessary updates. The systems controller must provide periodically information on the degree of compliance with the Policy, any threats detected and any incidents. This information is submitted to the Ethics, Compliance and ESG Committee, which in turn reports to the Ethics, Compliance and ESG Commission.

The systems controller also provides any needed technical assistance and specialized support to the Steering Committee, the Ethics, Compliance and ESG Committee, employees and even the Board of Directors when necessary.

The systems controller is also in charge of providing training so that all employees are aware of and understand the Policy and applicable measures.

Employees have the following responsibilities:

- Be aware of, understand and comply with the Policy.
- Maintain professional secrecy and confidentiality of all information handled in their workplaces.
- Urgent notification of the systems controller through established procedures of any potential incidents or breaches of security.

RELEASE AND DATE OF APPLICATION

This Policy was approved by Solaria's Board of Directors on 21 December 2020 and was released the following day.

COMMUNICATION OF THE POLICY

This policy will be made available to all employees of Solaria Group and to all the Company's interest groups through its corporate website (www.solariaenergia.com)

The policy will be subject to any communication and training initiatives that are considered necessary to make it known and understood.