Information Security Policy

Effective Date: 05/03/2026 DR.PO.1 V.1

Objective and Scope

The objective of this policy is to establish a framework for the continuous improvement of the Organization and its Information Security Management System, ISO 27000.

This policy applies to all systems, services, processes, employees, suppliers, and third parties with access to information processed by bheed or the environments used for its operation.

Responsible Parties

It is the responsibility of Mr. Sebastián Fuenzalida Farias, in his capacity as CEO, to provide the necessary resources and define the strategic guidelines for the ISMS.

The ISMS team is responsible for coordinating, supervising, and evaluating the implementation of controls and their effectiveness.

All employees and third parties are required to comply with this policy and its derived procedures.

Information Security Policy

Effective Date: 05/03/2026 DR.PO.1 V.1

bheed. develops, operates, and maintains a digital platform that manages the complete lifecycle of real estate projects. Given the critical role our platform plays for our clients, **Information Security** is a fundamental pillar of our operation.

With the purpose of protecting information assets and guaranteeing the continuity of our services, the organization establishes the following commitments:

1. **Protect the confidentiality, integrity, and availability** of our own information, as well as that of our clients, providers, and users.

2. **Ensure the operational continuity** of our digital platform and the support and maintenance services we provide to the real estate sector.

3. **Manage risks** related to cybersecurity, secure development, cloud operations, and technical support by applying controls proportional to industry threats.

4. **Comply with legal, contractual, regulatory, and statutory requirements** applicable to our operations and data processing.

5. **Implement secure development practices,** aligned with standards such as **OWASP** and **DevSecOps** best practices.

6. **Promote a security culture,** establishing clear responsibilities and ensuring the continuous training of our team members.

7. **Maintain and continually improve** the Information Security Management System (ISMS) by reviewing results, incidents, audits, risks, and opportunities to strengthen our services.

D **Change History**

Version	Type of Change	Author	Requester	Modification Date	Summary
V.0	Doc. Base	FSGI	Director	19/12/2025	Original Document
V.1	Doc. Base	FSGI	Director	06/03/2025	Original Document

E **Reviews**

Review and Approval	Final Approval
FSGI	Management