

DORAL

Renewable Energy

Doral's Data Security and Privacy Policy



Doral's Data Security and Privacy Policy

At Doral, we are committed to proper corporate governance, regulatory compliance, and ethical, responsible, and fair business conduct with all our stakeholders. In fulfilling these commitments, we adopt an exacting approach to securing the information that reaches us, handling it in a way that conforms with the expectations of the data provider. We set out these commitments as the basis for our policy, guided by relevant values from our Code of Ethics that serve as our moral compass for proper conduct on the topic:



Ensuring professionalism, excellence, and ethics

Aspiring for excellence

Investing in human capital

Belief in continuing education and development

Conduct according to business ethics, integrity, and fairness.

We support and promote employee development with the goal of preserving the highest level of professionalism, operational excellence and ethics in the Group's business and subsidiaries, enabling the application of knowledge and expertise in our areas of operation.



Succeeding together

Fairness in business

Foundation of trust

Cooperation

We affirm the importance of integrity and fairness while taking full responsibility in our areas of operation.

Our business is built on relationships of trust and integrity both in and outside of the Company and we hold all of our employees and representatives to high professional standards, requiring them to take responsibility both for their personal behavior and towards the organization.



Ensuring accuracy in our records and reports

We are committed to accurately recording all financial information and other business information related to the Company.

All our records and transactions comply with internal audits and accounting principles.

It is prohibited to record misleading or false information in the Company's records or reporting systems.

All information related to the Company is reported honestly, with the necessary accuracy and on timely dates, whether they are internal records, publicly available documents, including information submitted to governmental authorities.



Maintaining confidentiality and preventing use of insider information

The Company's stock trading policy prohibits buying or selling the Company's securities and/or shares in the Group's subsidiary companies and/or in a third party with which it has a business relationship, unless it is in accordance with the detailed procedure adopted by the Company on this matter.

An employee must not disclose or make implications regarding substantive non-public information to family members, friends, or others, either internal or external to the Company.

Employees are strictly prohibited from discussing financial, business-related, or other information about the Company with external parties unless they have been explicitly authorized to do so.



Ensuring proper disclosure

Our policy is to distribute substantive information regarding the Company's business only to employees authorized to use the information for a stated purpose.

We work to ensure complete, transparent, and comprehensible disclosure to provide a holistic picture of the Company's business and affairs.

Requests from media outlets, analysts, or shareholders regarding the Company are transferred to the Company secretary so that an authorized party can address such requests.

Doral supports progress towards the **United Nations' (UN) Sustainable Development Goals (SDGs)**. As part of our commitment, Doral works to promote SDG 8 – decent work and economic growth – to enable lasting, inclusive, and sustainable economic growth, as well as SDG 9 – building resilient infrastructure, promoting inclusive and sustainable industrialization, and fostering innovation.

This policy is presented as a public document and is a declaration of Doral's commitment to ethical, responsible, fair business conduct, which includes remaining highly attentive to the importance of strict data privacy and information security. Moreover, this document is intended to raise awareness of these issues among all stakeholders so that they may act accordingly. This document is relevant for all the Company's subsidiaries and joint ventures.

Implementation of information security and privacy procedures

At Doral, we have formulated and work to implement an information security procedure that defines the organizational, managerial, and professional guidelines for decision-making on topics of information security and data privacy. In addition, we built a structured system to manage both routine and extraordinary matters concerning the integration and adoption of information security aspects within the Company.

All employees are required to undergo an annual refresher training on information security procedures and aspects. In addition, external parties engaged by the Company undertake to maintain confidentiality of information, uphold our procedures regarding insider information, and information security.

Ensuring business continuity

In addition, considering the evolving landscape in Israel and globally, along with the necessity to address severe crises, we have deemed it appropriate to adopt a business continuity and disaster recovery procedure and plan. The plan was developed by the Company's CEO in collaboration with individuals in the Company's management and is guided by professional expertise and advice. This procedure was discussed and approved by the Company's Audit Committee. The objectives of the procedure include: definition of the course of operation when transitioning from routine to crisis situations, description of the conduct expected during a crisis until a routine state is reestablished, and determination of the designated roles to be fulfilled in a crisis; ensuring that all the Company's entities are familiar with the procedure so it can be effectively and efficiently implemented during a crisis; establishing the minimum level of business continuity preparedness required of the Company at all times, namely the resources deployed to operate critical processes, and the necessary personnel, infrastructure, information and

communication systems; and determination of the principles for practicing crisis preparedness.

The plan was devised based on a risk assessment, taking into account the criticality of the Company's processes and systems and their necessary availability. The objective was to address various aspects of information security, including safeguarding against unauthorized disclosure of sensitive information and processes. The Company's management or designated representatives are responsible for instructing all employees on the existence and implementation of the disaster plan.

Information security in relation to human resources

Doral's procedures on the topic include the establishment of processes for employee recruitment, onboarding, departure, and position changes. This includes addressing trust and reliability aspects, alongside the implementation of a managerial and operational framework to enhance information security awareness among our employees.

Information security guidelines and work with external entities

Relevant procedures include comprehensive guidelines concerning physical security, access controls, operational controls, information transfer, password management, proper use of the organization's assets, and backup and recovery protocols.

Additionally, we implement procedures regulating information security and privacy aspects in the context of our interactions with suppliers, service providers, and subcontractors to prevent mishaps and minimize exposure to risk when disclosing any company information or data with external parties. The procedures specify the range of measures and actions that should be taken when the Company engages with an external party.

Compliance with regulation

Activity in the field of renewable energy is subject to the directives of various regulatory bodies and institutions, such as: local authorities, the Electricity Authority, the Israel Electric Corporation, the Israel Securities Authority, the Israel Tax Authority, planning and construction bodies, various government ministries – the Ministry of Agriculture, the Ministry of the Interior and the Ministry of Defense, the Ministry of Environmental Protection, and decisions, procedures, and standards made by bodies acting on their behalf. Approvals are usually required prior to commencement of construction of the facility and its commercial operations. Doral's nature as a corporation, namely a

reporting corporation with global operations in the United States, Italy, Poland, Romania, and Denmark, makes us subject to the laws of those countries, as well as to the various environmental laws and their requirements, at the federal, state, and local levels. Despite the fact that we have extensively internalized relevant legislation, standardization, and regulation, we have adopted intra-organizational procedures to ensure the Company's proper management with **special emphasis on information security and privacy**.

Tracking, monitoring and reporting

At Doral, employees' reports of concerns regarding data leakage, infringement of privacy, and violations of the Company's Code of Ethics are handled with great sensitivity and care according to the procedures of the internal enforcement plan and policy documents, and thusly, we act immediately upon receiving knowledge of an incident. In addition, we report on our relevant activities in the context of our annual ESG report.

The dedicated manager responsible for managing the field at Doral acts in accordance with the Company's procedures in case of an incident, including through reporting, capturing lessons learned, and performing damage control.

Information security and privacy for all our stakeholders

At Doral, we work to raise awareness and promote relevant action among all our stakeholders. Special emphasis is placed on our engagement with the following stakeholder groups:

- **Our employees** – all company employees undergo required annual refresher trainings regarding information security aspects.
- **Business partners and suppliers** – encouraging suppliers and business partners to implement information security and privacy guidelines in their business operations. We also encourage supplier assessments of these aspects.
The Company requires external parties service providers, contractors, and consultants to sign a clause undertaking to maintain the confidentiality of information, uphold procedures to prevent sharing insider information, and for implementation of information security procedures as part of our engagement with them.
- **Subsidiaries and portfolio companies** – evaluation of ESG activities and encouraging growth of related activities, with a focus on information security and privacy.
- **Communities and social partners** – conduct according to work procedures that ensure the preservation of information and privacy of aspects in relationships between Doral and our community and social partners.

Implementation of this policy

- **Ongoing management of information security at Doral:** to implement this policy and engage in the ongoing management of these topics a dedicated manager has been appointed with responsibility for effectively implementing the Company's relevant procedures. This managerial position is responsible for implementation and enforcement of the relevant procedures, as well as for supervision and control of the Company's information security management, in addition to handling exceptional incidents and assessing damage caused by mishaps or crises, should they arise.
- **Ongoing implementation of the policy by a professional IT team at Doral:** The Company has within its ranks a professional IT team that is responsible for implementing the commitments detailed in this policy. The team is responsible for executing activities (utilizing processes, methods, and tools) and for implementing procedures and regulations related to information security within the domain of information systems. In addition, the team is responsible for reporting any information security incidents or related concerns for further handling, and for adopting processes and tools to implement the Company's information security principles.
- **Our managers and employees:** Doral's managers and employees are responsible for ongoing implementation of this policy in accordance with the Company's decisions.
- **Guidance and management of these topics by Doral's management:** Our management is committed to conducting dialogue in order to address incidents, should they arise, in addition to ensuring the effective implementation and assimilation of relevant procedures within the Company, including conducting hearings due to violation of this policy.
- **Guidance from Doral's Board of Directors:** Our Board of Directors is committed to guiding and monitoring the implementation of this policy through an annual discussion conducted by the Audit Committee. Any revisions to the Company's procedures on these topics requires the approval of the Audit Committee.

We invite our stakeholders to submit feedback or inquiries to the following email address: esg@doral-energy.com