

INFORMATION SECURITY POLICY

Monrol considers corporate information as a valuable asset. The environment, in which all kinds of corporate information and information belonging to Monrol and/or our business stakeholders used during the activities, are critical for our business and responsibilities and must be properly secured.

The concept of security consists of 3 components: confidentiality (prevention of unauthorized access to information), integrity (complete, accurate, not modified without authorization), usability (accessibility when necessary), and a security vulnerability that may occur in any of these main components can have a serious impact on the integrity and reputation of Monrol's business activities.

Regardless of their role and position, all Monrol employees and suppliers must comply with applicable legal regulations, policies, procedures as well as regulations, limit risks, and work within established good practices.

Monrol aims to protect the information and information assets of itself and its stakeholders with the Information Security Management System (ISMS). Monrol Management is committed to providing the necessary resources for the establishment, implementation, operation and continuous improvement of ISMS to achieve this objective.

Violation of information security policies and failure to implement necessary measures against risks may result in material and immaterial damage to Monrol. Therefore, information security and/or related policy/procedure violations identified as a result of surveillance, audit, and/or denunciation may lead to disciplinary penalties that may result in termination of employment and even juridical and criminal legal proceedings.

Monrol's Information Security Management System Policies/Procedures are applicable and compulsory for all Monrol employees using Monrol information or business systems, regardless of geographic location or business unit and whether full-time, part time, permanent, or contractual. All persons, such as third-party service providers and their affiliated support personnel who do not fall into this classification and who need access to Monrol information, must adhere to the general principles of this policy and other security responsibilities and obligations with which they must comply.