INFORMATION SECURITY MANAGEMENT POLICY

Scope

The purpose of this policy is to ensure the safeguarding and protection from all threats, internal or external, intentional, or accidental, of information managed within the scope of our activities in accordance with the guidance provided by the ISO/IEC 27001 standard and the guidelines contained in the ISO/IEC 27002 standard in their latest versions.
Cobraplast Management has defined and is committed to keeping active at all levels of its organization this Information Security Management Policy.
The Corporate Policy requires that, consistent with the corporate mission, the management of all business processes be set with the rules proper to the application of the TISAX Management System developed taking into consideration the ISO/IEC 27001 standard.
Information Security Management Policy means all the criteria, operating methods and technical and organizational tools designed to safeguard the confidentiality of information managed by the Company in the interest of itself, its Customers, Suppliers, and partners.

Scope of application

This policy applies indiscriminately to all bodies and levels of the Company.
The application of this policy is mandatory for all personnel and must be included in the regulation of agreements with any external party that, in any capacity, may be involved with the processing of information that falls within the scope of the TISAX Management System.
The information assets to be protected consist of all the information managed through the computer and manual systems, located in all the Company's locations, for which it is necessary to ensure:

- ✓ confidentiality: that is, the information must be accessible only by those who are authorized to access it.
- ✓ integrity: that is, to protect the accuracy and completeness of information and the methods for processing it.
- ✓ availability: that is, that authorized users can access the information and related assets when they request it.

Lack of adequate levels of security can result in damage to corporate image, lack of customer satisfaction, risk of incurring penalties related to violation of applicable regulations as well as economic and financial damage.
An adequate level of security is also basic for information sharing.
The Company identifies all security needs through risk analysis of its business assets to get proper knowledge about the level of exposure to threats. The risk assessment allows an evaluation of the potential consequences and damage that may result from failure to apply security measures to the information system and what is the realistic likelihood of implementation of the identified threats.
The results of this assessment determine the actions needed to manage the identified risks and the most appropriate security measures.
Our principles of information security management cover the following aspects:

a. <u>Always update asset inventory</u>
   Ensure a constantly updated list of company assets relevant to information management, and a responsible person must be identified for each. Information must be classified according to its level of criticality so that it is managed with consistent and appropriate levels of confidentiality and integrity.
b. <u>Updated information risk assessment</u>
   The information risk assessment shall be reviewed and updated at least once a year at the Management Review or if adverse events occur or if there is an adjustment to the asset inventory.

c. Secure systems access
   To ensure information security, all access to systems must be subject to an identification and authentication procedure. Information access permissions must be differentiated according to the role and positions held by individuals, so that each user can access only the information he or she needs and must be reviewed periodically.
d. Safe use of company assets
   Procedures must be established for the secure use of corporate assets and information and their management systems.
e. Ongoing staff training
   Complete awareness of information security issues must be encouraged in all personnel (employees and contractors) from the time of selection and throughout the employment relationship.
f. Timely management of adverse events
   To handle incidents in a timely manner, everyone must notify any security-related issues. Every incident must be handled as outlined in the procedures.
g. Adequate physical protection at corporate locations
   Unauthorized access to company premises and individual rooms where information is managed must be prevented, and equipment security must be ensured.
h. Management of contractual compliance with third parties
   Compliance with legal requirements and principles related to information security in contracts with third parties must be ensured.
i. Business continuity plan simulations
   A continuity plan must be prepared that enables the company to effectively cope with an unforeseen event, ensuring the restoration of critical services in a timeframe and manner that limits the negative impact on business operations.
j. Continuing IT security
   Security aspects must be included in all phases of installation, operation, maintenance, support and decommissioning of IT systems and services.
k. Continuous legislative update
   Compliance with the provisions of the law, statutes, regulations or contractual obligations and any requirements inherent to information security must be ensured, minimizing the risk of legal or administrative sanctions, significant losses, or image damage.
l. Periodic vulnerability scanning
   Periodic vulnerability scanning tests must be performed in infrastructure and applications to assess the resilience of systems to external attacks and detect any vulnerabilities and enable subsequent corrective actions.

Responsibility for compliance and implementation

Compliance with and implementation of the policies are the responsibility of:

- ✓ All personnel who, in any capacity, work with the company and are in any way involved with the processing of data and information that fall within the scope of the Management System. All personnel are also responsible for reporting anomalies and violations of which they may become aware.
- ✓ All external parties that have relationships and collaborate with the company must ensure compliance with the requirements contained in this policy.
- ✓ The Management System Manager who, within the framework of the Management System itself and through appropriate rules and procedures, must:
  - conduct risk analysis with appropriate methodologies and take all measures for risk management.
  - establish all regulations necessary for the safe conduct of all business activities.
  - verify security breaches and take necessary countermeasures and monitor the company's exposure to major threats and risks.

- organize training and promote staff awareness for everything related to information security.
- Periodically verify the effectiveness and efficiency of the Management System.

Any person (employees, consultants and/or external collaborators of the Company) who intentionally or attributable to negligence disregards the established safety rules and thereby causes damage to the Company may be pursued in the appropriate forums and in full compliance with legal and contractual obligations.

Review

Management will review, periodically and regularly or in conjunction with significant changes, the effectiveness and efficiency of the Management System, to ensure adequate support for the introduction of all necessary improvements and so as to encourage the activation of a continuous process by which control, and adjustment of the policy is maintained in response to changes in the business environment, business, and legal conditions.
The Management System Manager is in charge of the review of the policy.
The review should verify the status of improvement and corrective actions and adherence to the policy.
It should take into account all changes that may affect the company's approach to information security management, including organizational changes, the technical environment, availability of resources, legal, regulatory or contractual conditions, and the results of previous reviews.
The result of the review should include all decisions and actions related to improving the company's approach to quality and information security management.

Management Efforts

Management actively supports information security in the company through clear direction, overt commitment, explicit assignments, and recognition of responsibilities related to information security.
Management efforts are implemented through a structure whose tasks are:

- ✓ ensure that all objectives related to information security are identified and that they meet business requirements.
- ✓ establish corporate roles and responsibilities for developing and maintaining the TISAX Management System.
- ✓ provide sufficient resources for the planning, implementation, organization, control, review, management and continuous improvement of the TISAX Management System.
- ✓ monitor that the TISAX Management System is integrated into all business processes and that procedures and controls are developed effectively.
- ✓ approve and support all initiatives aimed at improving information quality and security.
- ✓ activate programs to spread information security awareness and culture.

C.O.O.
A. Lico