INFORMATION SECURITY POLICY

1. PURPOSE

Our company and its affiliates consider corporate and personal information as valuable and vital assets. Information is of critical importance for the sustainability of our business activities and must be properly protected. Our company commits to ensuring the protection of corporate and personal information within the framework of international standards, laws and regulations, including the Information Security Management System (ISO 27001), and to continuously improve, develop and review information security by managing existing and potential risks.

2. SCOPE

This procedure applies to all employees within **GÜRPİLSAN PLASTİK SAN. TİC. LTD. ŞTİ.**
Our Information Security Policy includes the standards that we have established through teamwork together with all our business partners, based on our fundamental principles and values.

3. RESPONSIBILITIES

The Management Representative is responsible for the implementation of this procedure. Records arising from the implementation of this procedure are kept in the HR Department.

4. INFORMATION SECURITY POLICY

As Gürpilsan Plastik and its employees, in order to manage all risks related to our business continuity and information assets, we adopt the implementation of the following matters as our policy:

1. Determining policies and procedures of our Information Security Management System in compliance with the requirements of international standards, primarily ISO 27001, preparing documented information and monitoring their up-to-date status,
2. Allocating resources for the establishment, maintenance and improvement of the Information Security Management System,
3. Ensuring compliance with legal regulations and contracts related to information security management systems,
4. Identifying risks related to business processes and ensuring their systematic management,
5. Ensuring the implementation of trainings that develop technical and behavioral competencies in order to increase awareness of information security and business continuity management systems,
6. Ensuring the continuation of the organization’s core and supporting business activities with minimum interruption and preventing potential interruptions through pre-planned practices,
7. Maintaining and improving the reliability of the organization by protecting the confidentiality, integrity and availability of assets,

8. Ensuring the management of security violations that the organization may face and applying disciplinary sanctions when necessary,
9. Minimizing unplanned interruptions,
10. Guiding and supporting individuals and encouraging continuous improvement in order to maintain the effectiveness of Information Security Management System practices,
11. Supporting personnel performing managerial duties to demonstrate leadership within their areas of responsibility and the importance they give to their work.

Our Information Security Policies are valid and mandatory for all personnel using company information or business systems, whether full-time or part-time, permanent or contracted, regardless of geographical location or business unit. All persons who do not fall into these classifications but require access to our information, such as third-party service providers and their affiliated support personnel, are required to comply with the general principles of this policy and adhere to other security responsibilities and obligations.

GP-PO-02 T 12.10.2024 Rev.00