Information Security Policy

1. The Object and Scope of Information Security

Information is critical in terms of maintaining our business activities and needs to be preserved properly. The security of our information assets is our priority to ensure the trust of the institutions and organizations served and the services we provide. MIP aims to minimize the risks and effects of these risks by applying the information security management system (BGYS) ISO 27001 standard and the effects of these risks that may arise on privacy, integrity and accessibility of corporate information.

MIP Information Security Policy; In order to maintain the reputation, reliability, information assets of MIP, and to continue with the least possible interruption of basic and supportive business activities aim to:

- Fully maintain the continuity of information systems,
- Maximize the level of compliance with employees to conscious, awareness and security requirements,
- Ensure that the compliance with the agreements made with third parties is fully established,
- Minimize information security violations and turn them into an opportunity to learn
- Fully compliance of information, access and storage of the laws,
- Application of the most up -to -date and effective technical security checks.

Each MIP employee is responsible for contributing to these goals.

2. Senior Management Commitment

In order to establish an effective information security management structure, the Board of Diretors approves the information security policy in which the information security strategy and roadmap is determined and requires its implementation.

MIP senior management undertakes to fulfill the following topics:

- Ensuring the confidentiality, integrity and accessibility of data and information systems,
- Determining and managing risks for information assets,
- Following the requirements of information security standards,
- Providing compliance with all legal legislation on information security,
- Evaluation of continuous Information Security and carry out continuous improvement opportunities in order to survive the management system.

- To carry out trainings to improve technical and behavioral competencies to raise awareness of information security.
- Preparing and publishing other sub -procedures/instructions/processes of this policies by the Information Technologies Group Directorate and Information Security Management Systems Committee.

3. All MIP Employees Responsibilities

MIP Information Security Policy is valid and compulsory for all employees independently of the geographical position or the business unit. MIP employee is obliged to comply with the policies and procedures published within the scope of the "Information Security Management System and to inform them of possible security violations and weaknesses.

In this context, MIP employee is responsible for;

- Complying with the information security policy and procedures announced to them
- Providing compliance with information security documents in documents such as processes, flows, instructions, guidelines and forms to be formed for their management of their process and systems.
- Receiving and evaluating all requests for information from third parties in written form
- Notifying the relevant unit in the incidents of informing the information security policies and/or procedures or information security violations.
- Not engaging in activities that may adversely affect the operation of information systems or endanger information security
- Notifying the Information Security unit about the update/improvement requests regarding the Information Security documents.
- Request access to information and corporate resources in line with business needs.
- Determining the access rights of the owned property and Personal Data, and who can be accessed on an administrator and user basis with what privilege.
- Responsible for observing and updating asset inventory.
- Ensuring that the assets they own are classified, updated and reviewed, including Personal Data.

MIP employee must also comply with the protection of confidential information and the MIP Code of Business Ethics. It undertakes to take the measures specified in the Personal Data Protection Law and to work in full compliance with the MIP Personal Data Protection Policy.

4. Third Parties Responsibilities

Non-MIP personnel, interns, outside users, regardless of their location or role, are responsible for conducting all business processes within MIP in a way that protects information.

Third-party service providers and support personnel who are not MIP personnel, but need access to MIP information, must adhere to the general principles and security obligations of this policy.

Information security regulations that must be complied with by third parties providing goods and services to MIP and their employees are determined by relevant contracts and protocols.

These include at least the following:

- To act in accordance with the MIP Policies and Procedures that regulate relations with third parties, especially the information security rules declared by contracts or protocols
- Not to share the information and assets of MIP with others without MIP approval and permission
- In case any information and assets belonging to MIP are requested, to submit this request in written form.
- To use the identities given to them by MIP in accordance with the agreements and instructions
- If the third party's employees working with MIP are to leave their own company /change their duties, to notify MIP on the same day and to have their authorization revoked
- Not to copy any data and software on MIP's devices, not to record the sound of the environment, not to take pictures or videos, not to share / act that may endanger data security or image without the approval and permission of MIP
- Performing system access at MIP locations under the supervision of Information Technologies teams.

5. Policy Ownership

Functional ownership of this policy and all standards and other supporting documents and training activities will be carried out by the Information Technologies Group Management.

Information Technologies Group Management is responsible for the following:

- Ensuring that this policy is supported by detailed standards, procedures, processes, and instructions when necessary, and that they are available as needed
- Periodically auditing and reporting compliance with all published policies/procedures/processes/instructions, especially the Information Security Policy.
- Ensure that policy requirements are communicated to all employees and all external party employee
- Establishing and maintaining the general management framework for information security
- Continually reviewing this policy to ensure it is updated and continues to reflect changes in the risk environment or threats facing MIP and all external parties business requirements or information and information systems.

6. Policy Compliance, Audit and Sanctions

Each unit manager is primarily responsible for taking the necessary measures and reviewing their systems to ensure compliance with the Information Security Policy.

Violations of the Information Security Policy may cause damage to MIP as a result of not implementing the necessary controls against risks, as well as criminal liability and compensation for material damages according to the Turkish Penal Code. Violations of the Information Security Policy detected as a result of both surveillance, audit and denunciation may result in internal disciplinary penalties, which can go up to termination of employment and even initiation of judicial and criminal legal proceedings.

Working together to implement this policy will help to continually protect our data and reputation and ensure the continued success of our business.