INFORMATION SECURITY POLICY

17.05.2018

CONTENTS

I. Definitions

Information Assets: means anything valuable for the organization (any information, software, hardware, person, process of the organization).

Information Security: means making the organization's information assets accessible only by authorized persons and they are protected from unauthorized changes, any such changes are recognized and information assets will be reachable whenever they are needed.

II. Scope

This policy covers all employees of the organization, the users that are accessing information systems as third parties, service, software or hardware providers that provide support to information systems and the visitors.

III. Objectives

The objective is to ensure confidentiality, integrity and accessibility of information and to protect the organization's information by determining the rules of information security that the employees of MAPFRE GROUP must comply when using the resources of MAPFRE GROUP.

IV. Commitments

- MAPFRE GROUP (Organization) places emphasis on the information security in accordance with its purposes, values and strategic goals.
- The organization's management aims:

    - To protect the reliability and image of the organization;
    - To be sure that executed contracts meet with the requirements of information security; and
    - To ensure that core and supporting operations of the organization do continue with minimum interruption.

For these purposes the organization undertakes to take the measures in order to ensure and maintain the confidentiality, integrity and accessibility of the organization's information assets.

- Information security risks are identified, evaluated and processed in accordance with the organization's risk management. Compliance and Risk Unit Management and Information Security Officer are responsible for management of risks.
- Anyone that uses the organization's information technologies infrastructure and accesses the information resources must:
    - Ensure confidentiality of the organization's information in case of personal and electronic communication and exchange of information with third parties;
    - Take security measures identified according to the level of risk;

    - Have information about breaches of information security, avoid any action that might cause a breach, and report any observed information security breach incident through the means identified and announced by the organization;
    - Not share internal information resources with unauthorized persons and not use them for actions in contradiction with applicable laws and regulations of the Republic of Turkey.
- The organization's employees and external parties, such as third persons, suppliers, customers, guests, etc. must comply with this policy as well as other policies, procedures and instructions issued for implementation of this policy.
- Environment and Security Committee is responsible to support and maintain the operation of information security infrastructure.
- The organization undertakes to provide "Information Security Awareness Training" to all employees in the form of e-training or classroom training, to improve information security continuously, and to meet applicable expectations of parties in relation with applicable legislations and regulations.
- If information security policies, procedures and instructions are not complied, the organization applies various sanctions, such as warning, reprimand, termination of employment agreement, etc. in accordance with the staff regulation.
- The organization's senior management is ready to provide any support for protection of information assets, creation of an information security awareness, development of a common corporate culture, taking necessary measures to identify risks and eliminate weaknesses, and execution of necessary sanctions in case of security breaches.
- The organization ensures compliance with the requirements of Information Security and Personal Data Protection LAW through internal and external audits, presentation of results of these audits to the management and taking necessary actions regarding these results. Applicable information security controls are also determined and managed with interested parties.

V. Approval and Reviews

This Information Security Policy was approved by the Executive Committee on 17.05.2018. It will be reviewed by the Information Security Officer at least on a yearly basis and will be amended by the Executive Committee if necessary. It may also be amended at any moment in order to be adapted to any significant changes that may affect its contents.