Information Security Policy

ARTICLE 1- PURPOSE

The Company considers the corporate information as an exceedingly valuable asset. The purpose of the Information Security Policy ("Information Security Policy" or "Policy") of the Company is to prevent the information security incidents or to minimize the risk of damage in order to ensure the business continuity of the Company and its subsidiaries and reduce the effect of the potential threats.

ARTICLE 2- SCOPE

The Information Security Policy is applied by the employees at all locations, and the suppliers / contractors within and outside the locations.

ARTICLE 3- INFORMATION SECURITY

Information is an asset that is of value for the company and therefore must be protected properly like the other important commercial and corporate assets. The information security protects the information from the areas of danger and threat in order to ensure the business continuity and minimize the losses. The information security is defined as the protection of the following information qualities in the Policy:

Confidentiality: Warranting that the information is accessible only to the persons who are authorized to access
Integrity: Ensuring the accuracy of the information and processing methods and the prevention of any unauthorized change to them
Accessibility: Warranting that the authorized users can access the information and associated sources most promptly when necessary

ARTICLE 4- INFORMATION SYSTEMS MANAGEMENT

The Information Systems Management includes the following:

(i) To establish, operate and manage the information systems,
(ii) To declare the information security policy to the personnel,
(iii) To implement, oversee and inspect the information security policy
(iv) To review the critical projects regarding putting the new information systems into use and to approve them by taking into account the manageability of the relevant risks,
(v) To bring the information security measures to an appropriate level, and to allocate adequate resources for the activities to be carried out for this purpose,
(vi) To review and approve the information security policies and all liabilities every year,
(vii) To identify the potential risks regarding the information systems and processes as well as its effects, and to realize the risk management that includes the definition of the activities for mitigating such risks within this framework,
(viii) To follow up and assess the incidents regarding the information security breaches every year,

(ix) To carry out activities and provide trainings in order to increase the awareness of all employees on information security,

(x) To incorporate the process and procedures established in order to manage the risks regarding the information systems into the organizational and managerial structure of the Company so as to actually function, and to carry out the oversight and follow-up processes with regard to their functionality,

(xi) To prepare a business continuity plan in order to ensure the continuity of all critical business processes according to the priorities of risks,

(xii) To ensure the development, operation and up-to-dateness of the controls regarding the measures that will ensure the confidentiality, integrity and accessibility of the information systems and the data available on them in order to be processed, forwarded and stored for the purpose of making sure that the security risks arising from the information systems are managed sufficiently, and to define the necessary managerial responsibilities,

(xiii) To identify the information assets owned by the Company and the persons who are responsible for these assets, to develop the inventory of these assets and ensure the up-to-dateness of this inventory, and to categorize the information assets by their degrees of importance,

(xiv) To ensure that the safe areas are protected by means of the necessary entry controls in order to ensure that only the authorized persons have physical access,

(xv) To design and implement physical safeguards against damages arising from fire, flood, earthquake, explosion, pillage and other natural or human-induced disasters,

(xvi) To establish and effectively manage control mechanisms in order to protect the networks against threats and to ensure the security of the systems, databases and practices using the networks,

(xvii) To take the necessary measures for ensuring the integrity of the transactions made through the information systems as well as the records and data,

(xviii) To take the measures that will ensure the confidentiality of the transactions made within the scope of the activities of the information systems, and of the data forwarded, processed and retained within the scope of these transactions,

(xix) To establish an effective audit trail recording mechanism for the use of the information systems by taking into consideration the complexity and extensionality of the risks, systems or activities on the information systems,

(xx) To conduct the works and procedures for outsourcing these services.

ARTICLE 5- EMPLOYEE AND THIRD PARTY LIABILITY

The compliance with the Information Security Policy is applicable and mandatory for all personnel who use the information or business systems of Akfen Holding and/or its subsidiaries, whether full-time or part-time, whether permanent or contracted, regardless of their geographical locations or business departments. The third party service providers and their inferior support personnel who are not included in these categorizations and who have access to the Company information due to the service they provide are obliged to act in accordance with the regulations and obligations under the Policy.

Those who use the Company’s information processing infrastructure and have access to its information resources:

(i) ensure the confidentiality, integrity and accessibility of the information belonging to the Company in personal and electronic communication.

(ii) take the security measures established according to the risk levels.
(iii) notify and report the information security breach incidents and take the measures that will prevent such breaches.
(iv) do not pass the internal information resources of the Company (notices, documents etc.) to third parties without authorization.
(v) do not use the information resources of the Company for the purposes of such activities that are in contrary to the legislation.
(vi) protect the confidentiality, integrity and accessibility of the information belonging to the investors, business partners, suppliers or other third parties.

ARTICLE 6- RISK MANAGEMENT

The risk management framework of the Company encompasses the identification, definition, assessment and processing of the information security risks, and the risk analysis and risk processing plan defines how to control the information security and service management risks.

ARTICLE 7- INSPECTION AND OVERSIGHT

The breaches of the Information Security Policy may cause damage to the Company and result in the legal, administrative and/or criminal liability of the Company as a result of the non-performance of the necessary inspections against risks. Accordingly, each department manager of the Company is responsible, at first degree, for taking the necessary measures in order to ensure the compliance with the Information Security Policy and overseeing the system apart from the inspection and oversight responsibilities clearly set forth in the Policy.