Information Security Policy

ARTICLE 1- PURPOSE

Akfen Construction recognizes corporate information as an extremely valuable asset. The purpose of the Information Security Policy of Akfen Construction (the "Information Security Policy" or the "Policy") is to prevent information security incidents or to minimize the risk of damage to ensure the business continuity of the Company and its subsidiaries and to reduce the impacts of potential threats.

ARTICLE 2- SCOPE

The Information Security Policy covers the information assets within the parent company Akfen Holding A.Ş. It is implemented by employees at all locations and by internal and external suppliers/contractors.

ARTICLE 3- INFORMATION SECURITY

Information, like any other important commercial and corporate assets, is an asset that has value for a company and thus required to be protected suitably. Information security protects information against dangers and threat areas to ensure business continuity and minimize losses. Information security is defined in the Policy as protecting the following information assets:

Confidentiality: means that information is accessible only by authorized individuals
Integrity: means ensuring that information and the processing methods are accurate and cannot be changed without authorization
Accessibility: means ensuring that authorized users can access to the information and relevant resources as quickly as possible in case of necessity.

ARTICLE 4- INFORMATION SYSTEMS MANAGEMENT

The Information Systems Management covers:

(i) Establishing, operating and managing the information systems,
(ii) Communicating the information security policy to the personnel,
(iii) Implementing, supervising and controlling the information security policy,
(iv) Reviewing critical projects related to the introduction of new information systems and approving these projects by taking the manageability of the risks into consideration,
(v) Upgrading the information security measures to a suitable level and allocating sufficient resources for the activities to be conducted for this purpose,
(vi) Reviewing and approving the information security policies and all responsibilities on a yearly basis,
(vii) Determining the potential risks related to the information security policies and processes together with their impacts and ensuring risk management that includes the identification of the activities to reduce these risks,

(viii) Monitoring and assessing the incidents related to the information security violations on a yearly basis,
(ix) Conducting activities and providing training to increase the information security awareness of all employees,
(x) Positioning the processes and procedures established for the management of the risks related to the information systems in a way that they will actually operate within the organizational and administrative organization of the Company and ensuring surveillance and follow-up of their functionality,
(xi) Preparing a business continuity plan to ensure the continuity of all critical business processes according to the risk priorities,
(xii) Developing, operating, updating and identifying the necessary administrative responsibilities for the controls regarding the measures intended to ensure the confidentiality, integrity and accessibility of the information systems and data that will be processed, transmitted and stored in the information systems in terms of ensuring that the security risks arising from the information systems are sufficiently managed,
(xiii) Determining the information assets owned by the Company and those responsible for these assets, creating an inventory of these assets and keeping the inventory up-to-date, classifying the information assets by their importance,
(xiv) Ensuring that secure areas are protected through necessary access controls to ensure that physical access is only made by the authorized individuals,
(xv) Designing and implementing physical protection against damages caused by fire, flood, earthquake, explosion, looting and other natural or man-made disasters,
(xvi) Establishing and efficiently managing controls to protect the networks against threats and to ensure the security of the systems, databases and applications that use the networks,
(xvii) Taking necessary measures to ensure the integrity of the operations, records and data created through the information systems,
(xviii) Taking measures to ensure the confidentiality of the operations conducted within the scope of the information system activities and the data transmitted, processed and stored as part of these operations,
(xix) Establishing an efficient audit trail recording mechanism regarding the use of the information systems by taking into consideration the complexity and scope of the risks on the information systems as well as the systems or the activities,
(xx) Conducting the necessary affairs and operations for the outsourcing of these services.

ARTICLE 5 - EMPLOYEE AND THIRD PARTY RESPONSIBILITY

The compliance with the Information Security Policy of Akfen Construction is valid and mandatory for all personnel that use the information or business systems of Akfen Construction and/or its affiliates, whether working on full-time, part-time, permanent or contracted basis, irrespective of the geographical location or business unit. Third party service providers and their relevant back-up personnel, who do not fall into the scope of these classifications and who have access to the information of Akfen Construction due to the services provided by them, are required to act in full compliance with the requirements and obligations described in the Policy.

Those who use the information processing infrastructure and access to the information resources of the Company:

(i) Ensure the confidentiality, integrity and accessibility of the Company's information in the personal and electronic communications.
(ii) Take the security measures determined according to the risk levels.
(iii) Report the information security violations and take the measures to prevent these violations.
(iv) Avoid providing internal Company information resources (announcements, documents, etc.) to non-authorized third parties.
(v) Avoid using the IT resources of the Company for the activities that violate the legislation.
(vi) Protect the confidentiality, integrity and accessibility of the information belonging to investors, business partners, suppliers or other third parties.

ARTICLE 6- RISK MANAGEMENT

The risk management framework of the Company covers the identification, assessment and processing of the information security risks, and the risk analysis and risk processing plan define how information security and service management risks are controlled.

ARTICLE 7- CONTROL AND SUPERVISION

The violations of the Information Security Policy may cause the Company to suffer damages as a result of the failure to implement the necessary controls against risks, and it may also result in legal, administrative and/or criminal liabilities. For this reason, in addition to the control and supervision responsibilities that are clearly regulated in the Policy; each department manager of the Company is primarily responsible for taking the necessary measures to ensure compliance with the Information Security Policy and supervising the system.