ENERJISA ENERJI INFORMATION SECURITY MANAGEMENT POLICY

As Enerjisa Enerji, we adopt the following principles regarding information security management in order to provide sustainable services with human, technology and solution-oriented in all areas of electrical energy industry.

- We ensure the security against unauthorized access and change of all industrial control systems, corporate information systems and information assets as a result of our activities which are used for delivering electric energy to our customers.
- We ensure the security of all kinds of personal data, commercial and financial information sources and processes that belongs to our Company, our stakeholders, our employees and our customers and take preventive measures to prevent leakage.
- We comply with all applicable laws, regulations, contractual obligations, industry standards and other relevant internal and external requirements about information security and make continuous improvements.
- In accordance with the principles of confidentiality, integrity and availability of our processes and information resources; we provide physical security, access management, auditability, and non-repudiation.

Enerjisa Enerji top management provides necessary resources, makes necessary assignments and guidance for the realization and sustainability of the Information Security Management System (ISMS).

Information Security, Risk and Compliance Group Management is authorized by the management to ensure the realization and sustainability of ISMS.

All Enerjisa employees are responsible for working comply with policies, procedures and instructions for ensuring Information Security.

By protecting the confidentiality, integrity and availability of the information assets and processes of our customers and company, we undertake to carry out the information security for the following purposes as all Enerjisa.

- We determine all roles and responsibilities related to information security with the support of management and coordination of all units.
- We identify, measure and evaluate objectives for information security.
- We analyze information security risks and opportunities, plan and implement remedial actions to address these risks and opportunities.
- We continuously carry out awareness and training activities, in order to increase the awareness of all employees and related stakeholders about their roles and responsibilities towards Information Security.
- We develop and maintain business continuity plans and systems to ensure the continuity of critical processes.
- We ensure that information security incidents are reported by all employees and related parties, take necessary controls to avoid a repetition of events with our cyber incident response teams.

- We ensure continuous improvement of the information security management system. We provide internal and external audits and management reviews for the continuous improvement of the system, take necessary actions by evaluating the risks and opportunities that occur with the determined objectives and findings.

ENERJISA ENERJI INFORMATION SECURITY MANAGEMENT APPROACH

Scope

Enerjisa Enerji nformation security management approach is set on Enerisa Enerji information security policy. The scope of Enerjisa Enerji Information Security Management Approach includes Enerjisa Enerji A.Ş, its electricity distribution companies (İstanbul Anadolu Yakası Elektrik Dağıtım A.Ş., Başkent Elektrik Dağıtım A.Ş., Toroslar Elektrik Dağıtım A.Ş.), incumbent retail companies (Enerjisa İstanbul Anadolu Yakası Elektrik Perakende Satış A.Ş., Enerjisa Başkent Elektrik Perakende Satış A.Ş., Enerjisa Toroslar Elektrik Perakende Satış A.Ş.). and Enerjisa Müşteri Çözümleri A.Ş. (all referred as "Enerjisa Enerji").

Data Security

- Information security requirements of Enerjisa Enerji are evaluated and the relevant actions are undertaken by the Cyber Security Group Management under the Enerjisa Enerji Information Technologies and Digital Business Management Department in order to meet the business needs and comply with laws and legal regulations. Enerjisa Enerji management provides the necessary support and make the necessary assignments to fulfill information security requirements.
- Enerjisa Enerji takes the necessary measures to ensure the confidentiality and security of customer information at the highest level within the framework of the relevant legislation, and in this direction, implements the measures and actions determined by the Company policies.
- Since data is one of the biggest values, at Enerjisa Enerji, the confidentiality, integrity and availability of data are of great importance. Necessary controls are carried out to ensure data security at every point where data is transmitted and stored. Enerjisa Enerji ensures that data can only be accessed by those required for business purposes on a need to know basis.
- Within Enerjisa Enerji, the information security management system is implemented with a defined risk management approach and implemented with information security policies, procedures, instructions and other documentation that include rules based on best practices. Relevant documentation is shared within Document Management System of the company and are made available to all Enerjisa Enerji employees. The purpose of information security documentation is to manage information security risks and to ensure that data is adequately protected. All Enerjisa Enerji employees are responsible for the implementation of these policies, in the operation of business processes and the use of the information assets they are responsible for.

Protection of Personal Data (KVVK)

- Enerjisa Enerji, as the Data Controller, processes personal data obtained from different channels (head office, region offices, customers, dealers, website, call center, etc.) verbally, in writing or through electronic media for the operation of its activities and continuity of its services.
- The personal data processed by the business units for the purpose of carrying out the necessary studies are securely stored in the electronic systems and physical environments used by Enerjisa Enerji.
- Enerjisa Enerji attaches importance to the security of personal data. Accordingly, it takes necessary and suitable technical and administrative security measures of which are compliant with relevant legislation to protect personal data against unauthorized access, damage, loss or disclosure.
- Any personal data requested for product and service sales / application through the Enerjisa Enerji website or existing in the Enerjisa Enerji system is never shared with third parties without the consent of the customer except the data transfers that do not require consent due to Article 5 of the Law on Personal Data Protection ("KVKK"). Assessments in means of Article 5 of KVKK are fulfilled by Regulation Legal Team.
- Third parties are prevented from accessing the information entered by Enerjisa Enerji customers through the website. In order to protect the confidentiality of personal information of customers, Enerjisa Enerji's system and access infrastructure has been kept at the most reliable level and necessary measures have been taken.
- Personal data whose purpose of use has expired and the legal storage period has expired, are deleted, destroyed or anonymized by Enerjisa Enerji in accordance with Act 7 of the KVKK.
- Enerjisa Enerji may work with third party companies when it deems necessary to provide certain services. It is ensured that the relevant organizations act in accordance with the security standards and the terms of Enerjisa Enerji. Enerjisa Enerji makes sure that data processors with whom it works attach importance to information security and act with the awareness of mutual responsibility, and it also guarantees this contractually. In line with the definition in the legislation, data processors only process personal data in accordance with the instructions of Enerjisa Enerji, within the framework of the contract concluded with Enerjisa Enerji and in accordance with the legislation.
- The copyrights of the information and materials on the Enerjisa Enerji website belong to Enerjisa Enerji. All copyrights, registered trademarks, patents, intellectual and other property rights regarding the information and materials on the Enerjisa Enerji website, other than those belonging to third parties, are reserved by Enerjisa Enerji.
- The rights of persons whose personal data are processed are regulated within the scope of Article 11 of the KVKK. Pursuant to the relevant article, data owners have the following rights over Enerjisa Enerji:

    a) Learn whether or not data are being processed,

b) Request relevant information if personal data related to him/her have been processed,

c) Obtain information as to the purposes of the processing of personal data and whether or not such data have been processed accordingly,

d) Know the third persons within or outside the country to whom personal data are transferred,

e) Ask for the rectification of any incomplete or inaccurate personal data process,

f) Ask for the erasure or destruction of the personal data within the framework of the conditions referred to in article 7,

g) Request the notification to third parties to whom the personal data have been transferred of operations carried out within the meaning of sub-paragraphs (e) and (f),

h) Object to any conclusion to the detriment of himself/herself, which results from analysis of the processed data exclusively by means of automated systems,

i) Request compensation for the damages incurred as a result of an unlawful personal data processing.

Enerjisa Enerji reserves the right to change and update the terms and conditions in this legal notice without the need for a prior notice.

Incident Response

Enerjisa Enerji has a Cyber Incident Response Team within the Cyber Security Group Directorate. All kinds of software, hardware and human-induced situations that disrupt the normal working order of Enerjisa Enerji business processes and negatively affect some or all of the information or industrial control systems are defined as information security incidents. Situations such as malware, phishing attacks, unauthorized access, cyber-attacks, data extraction are examined within the scope of information security incident management process. The application, system and access components of Enerjisa Enerji are continuously monitored using monitoring and detection tools that are deemed to be successful in the information security industry. It is ensured that incidents encountered within the scope of monitoring are evaluated, relevant actions are taken action and closed properly.

Technological developments and vulnerabilities in the world are followed by the Cyber Security Group Management through cyber intelligence services. Penetration tests are performed by independent teams once a year, and the safety of the applications and services of Enerjisa Enerji is ensured by implementing the secure development life cycle. In addition, vulnerability scans, source code analysis and maturity assessments are performed. The deficiencies that are identified after these studies are examined, monitored and the relevant actions are undertaken by the personnel of the Cyber Security Group Management. Necessary information has been shared on how Enerjisa Enerji personnel should report incidents and violations, and the actions to be taken after the notifications are defined within the processes.

Information Security Awareness

As data and data security are of great importance within Enerjisa Enerji, trainings are conducted in order to increase information security awareness. The completion rate of the trainings is monitored by the senior management in order to raise awareness within Enerjisa Enerji and to exhibit an integrated approach within the organization.

During the year, samples of phishing attacks are made monthly by the Cyber Security Group Management, the results are evaluated and reported to the senior management. A Cyber Security Newsletter is prepared and sent to all employees every two weeks and cyber security news from around the world are shared. It is ensured that each personnel sign the information security commitment and it is stated that information security issues are the responsibility of all personnel. Cyber security developments in the world are shared by the Cyber Security Group Management via announcement mails. Within the scope of awareness, clean table - clean screen policies are implemented, and policies are reminded with posters in the physical locations. In addition, information security reminders are constantly made on computer screen savers.

Licences and Certificates

The licenses and certificates of Enerjisa Enerji A.Ş and its distribution and retail companies on Information Security and systems are as below:

- Enerjisa Enerji A.Ş and its distribution and retail companies hold the ISO27001 Information Security Management System Standard license.
- Enerjisa distribution and retail companies hold the ISO20000 Information Technology Service Management Standard license.
- Enerjisa Enerji A.Ş retail companies hold the ISO22301 Business Continuity Management System certificate.

In addition, compliance with the Electricity Licensing Regulation, EKS Information Security Regulation, Electricity Distribution and Sales Call Center Service Quality Standards, EKS Security Analysis and Testing Procedures and Principles, which are subject to the Energy Market Regulatory Authority, is controlled periodically by Cyber Security Group Management.

Information Security at Third Parties

In case of working with third party companies in order to ensure the continuity and quality of the services provided by Enerjisa Enerji, confidentiality clauses are included in the contracts. In case of need for data sharing due to business requirements, only the necessary data is shared. Approval processes for the safe transfer of data are also put into use and ensure that only required data for the job is transferred. In order to protect such data in systems, security measures in accordance with international standards are taken in systems and applications. Critical suppliers are evaluated within the scope of information security according to the criteria determined in line with the annual plan. Actions to close the deficiencies seen in the results of the evaluations are followed by the Cyber Security Group Management.