ENERJİSA
Energy of Turkey

INFORMATION SECURITY MANAGEMENT POLICY

Publication Date: 23.02.2021

INFORMATION SECURITY MANAGEMENT POLICY

Enerjisa Enerji considers all the information that it collects and processes through all kinds of methods and that belongs to itself and its stakeholders as critical assets and takes utmost care and importance for its protection.

Accordingly, with reference to the ISO/IEC 27001 Information Security Management System standard, the Corporate Information Security Management System is effectively implemented within Enerjisa Enerji.

The main purpose of corporate information security is to ensure the confidentiality, integrity and availability of any information collected and processed by Enerjisa Enerji. Due to the nature of Enerjisa Enerji's corporate activities, the main goal of corporate information security is to prevent material and intangible losses that may occur and affect Enerjisa and its stakeholders, to early identify these losses if they occur and to minimize their possible effects by designing, operating, monitoring processes and taking precautions by continuously improving them.

Regardless of their positions or duties, all Enerjisa Enerji employees and related third parties comply with Enerjisa Enerji's practices, policies and procedures regarding information security. Violation of corporate information security policies and procedures may result in disciplinary action and criminal sanctions within the scope of the relevant legislation.

The manager of each unit is primarily responsible for taking all necessary measures in their areas of responsibility and controlling business activities in order to ensure compliance with corporate information security policies and procedures.

Enerjisa Enerji commits that it will meet the applicable requirements regarding information security institutionally, will ensure compliance with all kinds of legislations, laws, communiqués and similar regulations that Enerjisa Enerji is obliged to comply with, and will continuously improve its Information Security Management System.

INFORMATION SECURITY MANAGEMENT APPROACH

1.Scope

Enerjisa Enerji information 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").

2.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 fulfil 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 a critical asset, 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.
- 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.
- Within Enerjisa Enerji, the information security management system is implemented with a defined risk management approach and implemented in keeping 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.

3.Protection of Personal Data

- Enerjisa Enerji, as the Data Controller, processes personal data obtained from different channels (head office, region offices, customers, dealers, the website, call center, etc.) verbally, in writing or through electronic media with the consent of the customer (excluding the exceptions pursuant to Article 5 of the Law on Personal Data Protection (PDPL)) 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.
- Data owners are informed with clarification texts about the said data processing activities through our various channels on the purposes of processing, the security measures taken, the rights of the data owner and the application channels. In order ensure a lawful data processing, this clarification must be made to the data owner before the data is processed and if it is not within the scope of the exception in accordance with the PDLP, explicit consent must be obtained.
- Enerjisa Enerji attaches importance to the security of personal data. Accordingly, the Company prepares and updates policies and procedures for the protection of personal data, and 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 / applications 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 pursuant to Article 5 of the Law on Personal Data Protection (PDPL). The Regulation Legal Team performs an assessment to determine if consent is required pursuant to Article 5 of PDLP.

- 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 and legal storage period have expired, are deleted, destroyed, or anonymized in accordance with Article 7 of the PDLP.

- 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 rights of persons whose personal data are processed are regulated within the scope of Article 11 of the PDPL. Pursuant to the relevant article, data owners have the following rights over Enerjisa Enerji:

  i. Learn whether or not data are being processed,

  ii. Request relevant information if personal data related to him/her have been processed,

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

  iv. Learn what third parties their personal data have been transferred to both inside or outside the country,

  v. Ask for the rectification of any incomplete or inaccurate personal data process,

  vi. Ask for the erasure or destruction of the personal data within the framework of the conditions referred to in Article 7,

  vii. Request the notification of third parties the operations carried out (request for rectification of incomplete and inaccurate data, request for erasure or destruction of personal data) to whom personal data have been transferred,

  viii. Object to any conclusion to the detriment of himself/ herself as a result of the analysis of data processed exclusively by means of automated systems,

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

Applications made by data owners within the scope of this article are answered within the legal period by examining system records and customer documents.

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

4.Incident Response

Enerjisa Enerji has a Cyber Incident Response Team within the Cyber Security Group Management. All kinds of software, hardware and human-induced situations that disrupt the normal operations 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 as a result of these evaluations are examined, monitored and the relevant actions are undertaken by the Cyber Security Group Management.

In case of an information security incident or a vulnerability that may cause an incident, Enerjisa Enerji employees or related outsourced employees/external consultants are informed about the channels to make their notifications through. Reminders are also made at regular intervals. The process document for the actions to be taken after notifications is periodically reviewed and implemented. In addition, Information Security Undertaking document signed with the suppliers includes an article stating that that the suppliers should contact Enerjisa Enerji in case of an information security incident.

5.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 regular intervals 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. Again, e-learning trainings about information security are shared with all employees every two weeks. Within the scope of awareness, clean table - clean screen policies are implemented, and policies are reminded with posters in the physical locations.

All personnel are required to sign the information security commitment which states that information security issues are the responsibility of all personnel.

6.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, and compliance with Information and Communication Security Guide of the Presidency of the Republic of Türkiye, Digital Transformation Office is controlled periodically by Cyber Security Group Management.

7.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.