TÜRK TELEKOM

INFORMATION SECURITY POLICY

Türk Telekom evaluates and addresses the information security requirements that have been identified in order to meet expectations regarding business needs, laws and legal regulations with its Information Security Management System. Information security risks are determined, evaluated and monitored with the operation of the Information Security Management System. Türk Telekom Management makes appropriate assignments and provides the support necessary to ensure the effective operation of the Information Security Management System, and to this end Türk Telekom has established Information Security Policies to draw up a framework for the information security requirements, for which all parties contributing to Türk Telekom's operations are expected to adopt. The Information Türk Telekom Management ensures that independent reviews are conducted at least once a year, and that the results are reported for the purpose of monitoring the effective functioning of the Information Security Management System.

The Türk Telekom Information Security Policy is approved by the Board of Directors. The Company's Information Security Committee gathers at least once per year to evaluate all activities carried out and the reports prepared with regard to the Information Security Management System, to assign information security resources, to prepare a budget for its requirements and to evaluate the information security risk reports.

In addition, within the scope of the Personal Data Protection Law (No: 6698), the Personal Data Protection Committee has been established in order to provide control of all personal data processes within Türk Telekom and to fulfil legal requirements.

Protection of Personal Data

Personal data may be processed within the framework of the Protection of Personal Data Law No. 6698 (KVKK), Electronic Communication Law No. 5809, the regulations of the Information and Communication Technologies Authority, the Personal Data Protection Agency and other relevant legislative provisions. Pursuant to the relevant legislations, Türk Telekom takes all technical and administrative measures to ensure the appropriate level of security necessary to prevent the unlawful processing of personal data and to prevent unlawful access to the data and protect it.

Rights of the Data Subject with regard to the Processing of Personal Data

Pursuant to Article 11 of the KVKK Law, any person in connection with himself/herself may apply Türk Telekom to;

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.

Under the Law on the Protection of Personal Data No. 6698, all questions and requests related to personal data may be conveyed in writing to Türk Telekom at its address, at Turgut Özal Bulvarı 06103 Aydınlıkevler / Ankara (through the Notary channel etc).

Information Security Incident Management

Information Security Incident Management at Türk Telekom is performed by the Cyber Incidents Response Team (SOME), in line with the Information Security Incident Follow-up Procedure. SOME performs the follow-up of information security incidents through the Incident Response Form.

Measures are taken by deploying the necessary technologies to prevent and detect data violations. The violation incidents that have been detected by the Company are evaluated in accordance with the Türk Telekom Information Security Policies and Procedures and shared with the Ethics Committee and the National Cyber Incidents Response Centre (USOM), where necessary.

Policies and the Audit of the Systems

There are 22 policies regarding Türk Telekom's information systems management in order to develop, operate, ensure the update and determine the necessary managerial responsibilities for the controls with regard to the measures which will ensure the confidentiality, integrity and accessibility of the data that is stored in the information systems to be processed, transmitted and stored, and the information systems themselves. These policies are reviewed annually.

ISO/IEC 27001 certification audits of Türk Telekom are carried out once a year by the Turkish Standards Institute (TSI), which has international accreditation. In addition, Türk Telekom is audited by the Information Technologies and Communication Authority (ICTA), which is the telecommunication sector regulatory body assigned by the law. The implementation of the Information Security Policies and Practices by the related units within the Company is also periodically audited by the Information Security auditors and the Internal Audit teams.

Türk Telekom obtains the necessary permission from customers for the use of the data required to provide the services, for which it is authorized, to its customers, and only processes this data. In addition, data which is required in accordance with legal obligations within the scope of the telecommunication sector is kept. Access to all data within that scope is structured on a “Need to Know” basis, and only staff required to be party to such information as part of their duty are authorized to access to the data. In order to identify suspicious usage or usage of data which falls outside the stipulated purpose, access to this data is continuously recorded and audited.

Inter-system accesses, remote access to systems, access to databases, user identification processes and the reporting of request processes at Türk Telekom are undertaken with secure and controlled processes designed through the demand management systems. Security tests are performed on the systems before the projects go live and at certain intervals, and any security findings identified are resolved by the relevant teams. Security risks are minimized by separating the application layer, database layer, web layers through the layered structure planned in the network layer. Network-level security devices ensure that access is monitored in accordance with established rules. Within the scope of the Regulation on Network and Information Security, the processes for initiating and approving transactions to be performed on critical systems have been separated in accordance with

the article of the “Separation of tasks and environments”. Within the scope of access control, all systems are reviewed at least once a year in accordance with the Türk Telekom Group Information Security Policies and Procedures.

The systems that are engaged in the prevention of data leakage, either purposefully or inadvertently, from all kinds of channels through which critical data is processed and transferred, are used in Türk Telekom’s networks by observing the movements of end users. Anonymization, masking of critical / personal / confidential data, and the related user authorizations are performed in the databases in order to meet the Law on Protection of Personal Data requirements and to prevent unauthorized access to confidential data.

The one-year audit plan, which principally covers technology processes and is drawn up based on the risk assessments performed at the end of each year, is approved by the Audit Committee formed within the Board of Directors. The Türk Telekom Internal Audit Department is authorized to perform the audit plan. In recent years, Information Security has been repeatedly determined as one of the most critical fields among the subjects handled during the risk assessments carried out within this framework. Accordingly, the Türk Telekom Internal Audit Department’s audit plans cover the Information Security Policies and Systems every year. In addition, in accordance with generally accepted auditing principles, within the framework of the methodologies used, the Internal Audit Department provides reasonable assurance for the audits in the fields related to Information Security within the Türk Telekom Group.

Information Security at Third Parties

Türk Telekom’s third party information security policy is signed by third parties and their compliance is audited. Approval processes are also put in place pertaining to the safe transfer of data and ensuring that no more data than is required by the work is transferred. In order to protect such data in the systems, security measures meeting international standards are put in place in the systems and applications. Under the Law on Protection of Personal Data, relevant Information Texts were prepared by Türk Telekom.

In all contracts, the third party Information Security Policy is signed by the companies; within the scope of the related work, the Security Agreement is signed by each employee of the Company that will provide services to Türk Telekom. With the aforementioned Policy and Agreement, the measures to be taken in order to protect confidential or sensitive data of Türk Telekom are defined and the responsibilities are specified.

Türk Telekom has authorized dealers that process customer data as third parties. The Information Texts have been distributed to be displayed in visible areas at all dealers. Consent documents were prepared addressing the customers and dealer employees for all work processes requiring explicit consent, and the dealers are required to obtain such consents in all necessary cases. In addition, business partner and supplier contracts are reviewed and revised in accordance with the Law on Protection of Personal Data and related legislation. Furthermore, necessary trainings are provided, announcements are conveyed and audits are carried out for business partners and the dealers within the scope of the protection of personal data.

Employee Training Programs Related to Information Security and Confidentiality

Information Security and Business Continuity training programs are provided to personnel, through both in-class and e-learning programs. Information security commitment is signed by the personnel. In addition, information e-mails concerning information security issues are regularly sent to personnel.

The regular online training programs conducted include the following topics:

- The date and legal basis of personal data processing
- The main responsibilities of Türk Telekom in this regard
- Personal Data Processing Inventory and VERBIS
- Rights of the person concerned
- Data storage times and deletion / destruction
- Penalties set out by relevant laws and regulations
- Special measures to be taken in Türk Telekom's business processes
- Actions to be taken specific to the personal data with special attributes
- Information Security Awareness
- Business Continuity

Information Security Certifications

Türk Telekom holds the ISO 27001 certificate covering fixed and mobile networks. Within this scope, Information Security Internal Audit activities are carried out on an annual basis and action assignment and follow ups are performed in accordance with the audit results. In addition, all employees are assigned Information Security Awareness trainings periodically within the scope of the ISO 27001 standard.

In addition, Türk Telekom holds PCI-DSS certification under the mobile network. In this context, vulnerability and penetration tests of the systems are performed at certain intervals. Within the scope of the PCI-DSS, awareness trainings as required by the standard are periodically provided to the related employees.