INFORMATION SECURITY POLICY

1. Purpose: The purpose of this policy is to define the senior management's approach and goals and to inform all employees and interested parties in order to prevent violations related to law, legal, regulatory or contractual obligations and any security requirements.

2. Scope: This policy protects the electronic information assets obtained from the logistic, storage, accounting, finance, quality assurance, purchasing, human resources, law, sales, marketing, internal audit and data processing activities related to the commercial activities carried out within the Company and these transactions. covers the information security processes used to process, store, protect, protect privacy and integrity of personal data held within the company.

2.1. Internal Coverage

Administration, structure, roles and obligations related to the organization;

2.1.1. The departments within the scope of the Company's Top Management are: Financial and Administrative Affairs, Purchasing, Finance, Computing, Corporate Communication and Business Development, Human Resources, Quality, Export, Import, Logistics, Law, Internal Audit, Sales, Marketing

2.1.2. Roles and responsibilities in job descriptions stated in the General Management Organizational Chart.

2.1.3. Policies, procedures, goals and strategies to be implemented;

2.1.3.1. Information Security Management System Policy,

2.1.3.2. All Information Security management systems procedures,

2.1.3.3. Annual Information Security management systems targets determined by the management,

2.1.3.4. Skills understood in terms of resources and knowledge (eg principal, time, people, processes, systems and technologies),

2.1.3.5. Management Representatives and Information Security Management System team appointed by management for the establishment, operation and maintenance of the Information Security Management System,

2.1.3.6. Relations with internal stakeholders and their perceptions and values, the culture of the organization, standards, guidelines and models adapted by the organization; covers its form and width.

2.2. External Scope

2.2.1. International, national, regional or local, social and cultural, political, legal, legislative, financial, technological, economic, natural and competitive environment,

2.2.2. Global Competition Law, Policies and Procedures,

2.2.3. Confidentiality of supplier and customer data,

2.2.4. Quality Orientation,

2.2.5. Relations with stakeholders that have an impact on the organization's goals and their perceptions and values;

2.2.6. All Company employees, including Senior Management, to ensure customer satisfaction,

2.2.7. All relevant legal legislation, regulator, contractual conditions, standards,

2.2.8. Product certification with TSE and other organizations is external coverage.

3. Definitions

3.1. ISMS: Information Security Management System.

3.2. Inventory: All kinds of information assets that are important for the company.

3.3. Top Management: The Company is the Top Management.

3.4. Know-How: Competence to do something.

3.5. Information Security: Information, like all other corporate and commercial assets, is an asset that has value for a business and therefore must be properly protected. Within the company, know-how, process, formula, technique and method, customer records, marketing and sales information, personnel information, commercial, industrial and technological information and secrets are accepted as SECRET INFORMATION.

3.6. Confidentiality: The display of the content of the information is restricted to access by only those who are allowed to view the information / data. (Example: By sending encrypted e-mail, unauthorized persons can be prevented from reading e-mails even if the e-mail is intercepted - Registered e-mail - KEP)

3.7. Integrity: It is the ability to detect unauthorized or accidental modification, deletion or additions, and to ensure the detectability. (Example: Storing the data stored in the database with summary information - electronic signature - mobile signature)

3.8. Accessibility / Availability: The asset is ready to be used whenever it is needed. In other words, the systems are always in service and the information in the systems is not lost and is constantly accessible. (Example: Uninterruptible power supply and use of redundant power supply on the chassis to prevent servers from being affected by power line surges and power outages - UPS). It will be used as "Accessibility" in this policy.

Information Asset: These are the assets that are important for the Company to carry out its activities without disruption. Information assets within the scope of the processes subject to this policy are:

3.9.1. All kinds of information and data presented in paper, electronic, visual or audio media,

3.9.2. Any software and hardware used to access and change information,

3.9.3. Networks that enable the transfer of information,

3.9.5. Departments, units, teams and employees,

3.9.6. Solution partners,

3.9.7. Services, services or products provided by third parties.

4. Responsibilities The qualifications and competencies of the duties and responsibilities of which are determined are defined in the job descriptions. The IT Team and Management Representative are responsible for maintaining and developing information security related activities. ISMS Team and Management Representatives were appointed by Senior Management. BGYS representatives were determined from the departments within the scope. As a member of the ISMS team, assignments were made on a name basis.

4.1. Management Responsibility

4.1.1. The Company Management undertakes that it will comply with the Information Security System that has been identified, put into effect and is being implemented and that it will allocate the necessary resources for the system to operate efficiently and that the system will be understood by all employees.

4.1.2. During the installation of ISMS, it is appointed by the letter of the ISMS Management Representative. When necessary, the document is revised by the senior management and the appointment is made again.

4.1.3. Managers at the management level help the lower-level personnel to give responsibility and set an example for security. The understanding, which starts and applies from the upper levels, must go down to the lowest level personnel of the company. Therefore, all managers support their employees to comply with the safety instructions in writing or verbally and to participate in the works on security issues.

4.1.4. Senior Management creates the budget required for comprehensive information security studies.

4.2. Management Representative Responsibility

4.2.1. Planning the ISMS (Information Security Management System), determining the acceptable risk level, determining the risk assessment methodology,

4.2.2. Providing the necessary resources for supportive and complementary activities in ISMS setup, providing / improving user capabilities and awareness

4.2.3. formation, trainings, communication, documentation requirements,

4.2.4. Execution and management of ISMS practices, ensuring continuity of evaluations, improvements and risk assessments,

4.2.5. Evaluation of ISMS and controls through internal audits, targets and management review meetings,

4.2.6. It is responsible for maintaining the existing structure and ensuring continuous improvements in ISMS.

4.3. ISMS Team Members Responsibility

4.3.1. Conducting asset inventory and risk analysis studies related to its departments,

4.3.2. Informing the Management Representative for a risk assessment when there is a change in the information assets under his responsibility that will affect the information security risks,

4.3.3. Ensuring that department employees work in accordance with policies and procedures,

4.3.4. Raising awareness within the scope of ISMS regarding its departments, ensuring communication, providing documentation requirements,

4.3.5. It is responsible for maintaining the existing structure and ensuring continuous improvements in ISMS.

4.4. Internal Auditor Responsibility It is responsible for conducting and reporting the audit activities in the internal audits assigned in line with the internal audit plan.

4.5. Department Managers Responsibility They are responsible for the implementation of the Information Security Policy and ensuring that employees comply with the principles, ensuring that third parties are aware of the policy and reporting security violations related to the information systems they notice.

4.6. Responsibility of All Employees

4.6.1. To carry out its works in accordance with information security objectives, policies and information security management system documents,

4.6.2. It monitors information security targets related to its own unit and ensures that the targets are achieved.

4.6.3. Paying attention to and reporting any information security vulnerabilities observed or suspected in systems or services,

4.6.4. In addition to service contracts (consultancy etc.) with third parties that are not responsible for Purchasing, they are responsible for securing confidentiality agreements and providing information security requirements.

4.7. Responsibility of Third Parties It is responsible for knowing and implementing the information security policy and complying with the behaviors determined within the scope of ISMS.

5. Information Security Objectives The Information Security Policy is to guide the Company's employees to act in accordance with the security requirements of the company, to increase their awareness and awareness, and to ensure that the basic and supportive business activities of the company continue with minimal interruption, to maintain its reliability and image, and to maintain the third It aims to protect the physical and electronic information assets that affect the entire operation of the company in order to ensure compliance with the contracts signed with the parties. The targets determined by the management are monitored in determined periods and are reviewed at the Management Review meetings.

6. Risk Management Framework The Firm's risk management framework; It covers the identification, assessment and processing of information security risks. Risk Analysis, applicability statement and risk processing plan define how information security risks are controlled. ISMS Execution and Management Committee is responsible for the management and realization of the risk management plan. All these studies are explained in detail in the asset inventory and risk assessment instruction.

7. General Principles of Information Security

7.1. Details of the information security requirements and rules outlined by this policy, Company employees and third parties are responsible for knowing these policies and procedures and conducting their work in accordance with these rules.

7.2. Unless otherwise specified, these rules and policies are essential for all information stored and processed electronically and processed, and for the use of all information systems.

7.3. The Information Security Management System is configured and operated on the basis of the TS ISO / IEC 27001 "Information Technology Security Techniques and Information Security Management Systems Requirements" standard.

7.4. It carries out the implementation, operation and improvement works of ISMS with the contribution of the related parties. ISMS Management Representative is responsible for updating ISMS documents when necessary.

7.5. The information systems and infrastructure offered to the employees or 3rd parties by the company and any information, documents and product produced by using these systems belong to the company unless there are legal provisions or contracts requiring otherwise.

7.6. Confidentiality agreements are made with employees, consultancy, service procurement (Security, service, food, cleaning company etc.), Supplier and Trainee.

7.7. Information security controls to be applied in recruitment, job changes and turnover processes are determined and implemented.

7.8. Trainings that will increase the awareness of information security of employees and contribute to the functioning of the system are regularly given to existing company employees and new employees.

7.9. All actual or suspicious violations of information security are reported; Incompatibilities that cause violations are identified, measures are taken to prevent their repetition by finding the main causes.

7.10. Inventory of information assets is created in line with information security management needs and asset ownerships are assigned.

7.11. Corporate data are classified and the security needs and usage rules of data in each class are determined.

7.12. Physical security controls are applied in parallel with the needs of assets stored in safe areas.

7.13. Necessary controls and policies are developed and implemented against physical threats that they may be exposed to both within and outside the firm for information assets of the firm.

7.14. Procedures and instructions regarding capacity management, relations with third parties, backup, system acceptance and other security processes are developed and implemented.

7.15. Audit log generation configurations for network devices, operating systems, servers, and applications are adjusted in parallel with the security needs of the respective systems. Audit records are protected against unauthorized access.

7.16. Access rights are assigned as needed. The safest possible technologies and techniques are used for access control.

7.17. Security requirements are determined in system supply and development, and it is checked whether security requirements are met in system acceptance or tests.

7.18. Continuity plans are prepared for critical infrastructure, and maintenance and application is carried out.

7.19. Necessary processes are designed to comply with laws, internal policies and procedures, and technical security standards, and compliance is ensured through continuous and periodic surveillance and inspection activities.

8. In case of violation of the Policy and Sanctions If it is determined that the Information Security Policy and Standards are not complied with, the sanctions determined in the relevant articles in the contracts that are valid for the 3rd Parties are applied according to the Disciplinary Directive and Procedure for the employees responsible for this violation.

9. Management Review Management review meetings are held by organizing ISMS Quality Management Representative with the participation of Senior Management and Department managers. These meetings, where the suitability and effectiveness of the Information Security Management System are evaluated, are held at least once a year.

10. Updating and Reviewing the Information Security Policy Document ISMS Management Representatives are responsible for ensuring the continuity and review of the policy document. Policies and procedures should be reviewed at least once a year. Apart from this, it should be reviewed after any changes that would affect the system structure or risk assessment, and if any change is required, it should be approved by senior management and registered as a new version. Each revision should be published in a way that all users can access.