yuchisoft
software & technology

Information Security Policy

EYS.P0.01 Rev:00 Release Date:02.01.2023

CONTENTS

1- INTRODUCTION

The Information Security Policy created within the scope of TS ISO/IEC 27001 ISMS has been prepared as a guide that will include the purpose, scope, content, methods used, participants, duties and responsibilities, and rules to be followed for the information security management system carried out within the institution. This policy document is a parent document that also includes the information security policy and detailed usage policies. Approved and published by the management. It is regularly reviewed by management.

PURPOSE

TS ISO/IEC 27001 Information Security Management System compliance studies have been initiated in order to ensure, develop and increase the security of the information our Company has regarding the activities it carries out. Another important feature of these studies is to ensure the continuity and continuous improvement of the system to be established..

Information security is not only the responsibility of information technology employees, but is a job that can be achieved with the participation and compliance of all employees of our Company. However, it is not just about taking technical measures related to information technologies and running the processes. This system includes the selection, implementation and continuous measurement of various controls with the risk management method on many issues, from physical and environmental security to human resources security at the lower layers, from communication and communications security to information technology security at the upper layers. Implementation detail information is included in the system documentation, relevant procedures, guides, plans and reports.

Protection of our Company's Employees, Customers, Financial, Supply and End User data:

SCOPE

Our Company's Management System and Environmental Scope are defined in the Scope of the Organization document.

THE PARTIES CONCERNED

In the activities carried out within the scope; The relevant parties of the ISMS established in our Company due to legal and regulatory obligations related to the activity are listed in the Relevant Parties' Needs and Expectations document.

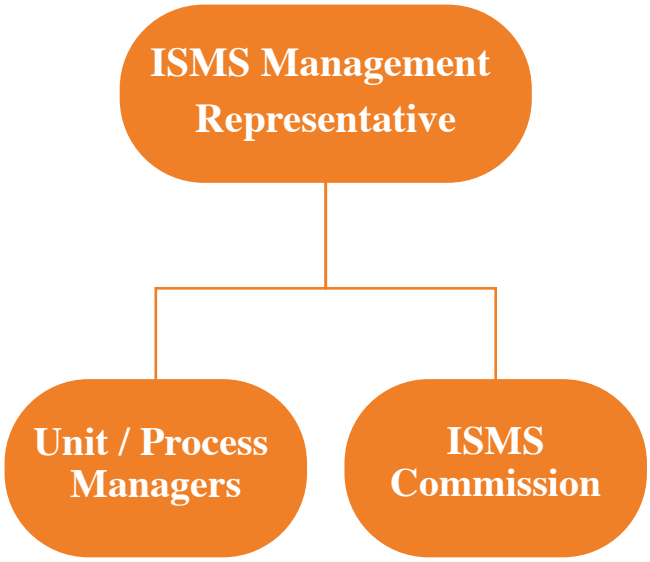
2- INFORMATION SECURITY GOALS AND PRINCIPLES

In the assets included within the scope of information security management and all processes related to them; Various activities are carried out to take measures to comply with the principles of Confidentiality, Integrity and Accessibility. These activities are included in the Asset - Resource Inventory Plan. Our Company's Information Security Management System aims to keep the risk level for each asset below the acceptable risk level through Risk Management. Risk management and implementation of controls is a continuous activity. For this reason, it is aimed to make improvements for risks that will fall below the acceptable risk level.

Our company aims to achieve the following goals with ISMS:

ISMS TARGET	PERFORMANCE CRITERIA
1. Increasing information security awareness of all employees.	At least 1 ISMS training number per year
2. Keeping the successful backup rate at a certain level.	At least 95% successful backups per year
3. Keeping the successful backup rate at a certain level.	95% annual number of successful restores from backup
4. Keeping the anti-virus rate installed on all server and user systems at a certain level.	100% AV installed system rate
5. Meeting the SLA target on the main internet connection.	99% annual up-time
6. Keeping the number of BG Commission meetings at a certain level.	At least 3 meetings annually
7. Keeping the number of internal audits at a certain level.	At least 1 internal audit annually
8. Keeping the number of management reviews at a certain level.	At least 1 review per year
9. Keeping the number of risk management plan reviews at a certain level.	At least 1 review per year

3- INFORMATION SECURITY ORGANIZATION AND INFRASTRUCTURE



ISMS JOB DESCRIPTIONS AND AUTHORIZATIONS

Task : ISMS Sponsor – Senior Management

Authorities and Responsibilities :
Providing the necessary resources for the establishment and operation of ISMS
Approving the control choices offered by the unit
Approval for investments and changes
Chairing regular ISMS Review meetings
Organizing encouraging activities for the participation of corporate employees
Assigning and authorizing the ISMS unit with the ISMS manager
Determining ISMS risk acceptance criteria and approving the risks to be accepted
Presiding over the ISMS Commission or delegating power to the Management

Task : Management Representative

Authorities and Responsibilities :
Managing ISMS preparation, operation, continuity and improvement activities
Preparing ISMS policies and procedures and revising them when necessary
Ensuring that the records required by ISMS are kept by establishing the registration system
Ensuring that risk management activities are carried out continuously and properly
Measuring the effectiveness of controls
Keeping the threat and vulnerability database up to date and managing changing risk
Managing audit and internal audit planning and implementation activities
Providing change and configuration management activities
Leading the emergency response team
Organizing YGG meetings
Informing senior management about the studies carried out within the scope of IMS

Competencies	:	Graduated from a Universty Intermediate English knowledge Having received chief auditor training Minimum 2 years professional supervision Having established or managed an ISMS System
Task	:	ISMS Commission
Authorities and Responsibilities	:	To make decisions regarding the establishment of ISMS and the execution of the work within the framework of the provisions of TS ISO / IEC 27001 Information Security Management System Standard.
Competencies	:	Commission Chairman University Graduate Intermediate English knowledge Minimum 2 years professional supervision Prone to teamwork, organized Having received basic and documentation training on ISMS
Task	:	Unit / Process Managers
Authorities and Responsibilities	:	Participating and taking part in ISMS internal audits Implementing and monitoring ISMS control practices Doing your part in emergency action plans Assisting BG manager with planning and reporting
Competencies	:	Graduated from a Universty Intermediate English knowledge Minimum 2 years professional supervision Prone to teamwork, organized Having received basic and documentation training on quality and ISMS

PARTICIPATION IN ISMS APPLICATIONS

All employees of our company must comply with the terms and rules specified in this policy. It should assist the information security team in fulfilling its ISMS-related duties. Each employee is responsible for complying with the risk management activities carried out to achieve the objectives specified in this policy published by the management and the rules specified in the information security guide. Those who do not comply with the instructions and controls will be dealt with according to the disciplinary process specified below.

Each employee is responsible for the control and confidentiality of the information assets under his/her responsibility and management. It is among the duties of every employee to participate in the necessary analyzes and implement controls for these assets within the framework of the risk management methodology chosen by our institution. Employees are obliged to monitor the adequacy and efficiency of the applied controls and to report security breach incidents or threats and weaknesses that may lead to a breach, without delay, in accordance with the breach incident procedure specified below.

No hardware, software or physical changes should be made to information assets without the knowledge of information security managers. The ISMS team manager must be notified about the changes that need to be made, and a record must be kept for the changes in accordance with the change management procedure specified below. In addition, records regarding changing the asset properties specified in the configuration management procedure must be created.

ISMS YGG MEETING

Management Review Meeting; It is a meeting held at least once a year, where senior management and ISMS Commission members are present, where the suitability, efficiency, functionality of risk management, audit results, corrective and remedial activities of the ISMS are discussed and evaluated. The ISMS Meeting can also be held following the YGG meeting or together with the YGG meeting. At this meeting, management evaluates risk acceptance criteria and related resource needs. The efficiency of studies, risk assessment and processing activities is also examined at this meeting.

Inputs and outputs used in these meetings are recorded using the Meeting Minutes Form in accordance with the standard.

4- RISK ASSESSMENT AND RISK MONITORING

Within the scope of the ISO 9001:2015 Quality Management System and ISO 27001:2013 Information Security Management System Standard harmonization studies carried out within our company, the Risk Assessment and Risk Processing process is defined in the Risk Management Procedure. In this document, for risk management, identification of informational assets and their evaluation, Risk Assessment methodology, Risk Processing steps and the rules to be followed in these steps are defined.

5- SOA-DECLARATION OF APPLICABILITY

Risk treatment options can be selected from the checklist in the control group given in ANNEX-A of the standard. The purpose of choosing each of the selected controls, the content of the control, the way the control is implemented and, if not, the reason why it is not implemented are stated in the document called SOA (Statement of Applicability). SOA is classified as confidential information and is only accessible to the ISMS Unit and ISMS Commission.

Information security objectives and practices are detailed in SOA. The Risk Management plan and SOA are parallel documents and are reviewed together. The names of the controls selected in the risk treatment plan, or if they are selected from ANNEX-A, are referred to the control number as A.X.X, while the control is detailed in the SOA. All applied and to be implemented controls are recorded in the SOA. This document provides a cross-check with the Risk Management plan to ensure that no controls are missed.

6- INFORMATION SENSITIVITY AND RISKS

Our Information Assets

Desktop computers, laptops, External and Portable Hard disks, USB Memory Sticks, Servers, CD and DVD etc. All data in electronic or written-printed media such as data in the media, documents, folders and file cabinets, servers, or in the transmission media (internet, e-mail, telephone, etc.) are defined as information assets for our Company.

Asset Classification

Each employee within our company has classified the information he or she uses or produces within the framework of this classification. According to this classification;

Publicly available information, all kinds of printed or digitally stored application forms, specifications, etc. published on the website or that are not harmful to be given or disclosed to third parties. information.

Company specific information, it is information that is only available to employees within the company. It is information that should not be accessed by unauthorized persons outside the institution.

Classified information, it is the most valuable information whose integrity and confidentiality are most critical. Protecting this information is extremely important both in terms of business continuity and legal requirements. Control and protection methods are defined and managed for all assets in the confidential information class.

Information Classification Guide

In order to ensure the Confidentiality, Integrity and Accessibility of Information in our Company, the information produced within our Company is classified as detailed in the table below.

Information generated during defined processes within our Company is classified according to its level of importance as Public, Personal, Internal Use, Company Specific and Confidential. Necessary explanations regarding classification and storage locations are explained in the table below.

INFORMATION CLASS	EXPLANATION	STORAGE LOCATION
PUBLIC	It is general or company-specific information that is safe for third parties to know. This information is available to customers, business partners, suppliers and the public. Availability of this information is important.	On cabinets and outside cabinets, on websites, on all kinds of media.
SPECIAL FOR THE COMPANY	This information is for the use of company employees. Accessibility and integrity are at the forefront. Information shared by departments among themselves falls into this class.	Department's common cabinets
PRIVATE	It is the most critical information, only accessible by management and relevant personnel specific to the work performed. It is very important for the institution that such information is not accessed, disclosed or shared without authorization. Privacy is at the forefront.	Kept in closed rooms/cabinets/drawers or personal computers controlled by the preparer.

Critical assets

Employees, servers, desktop and laptop computers, document cabinets, company information such as forms, plans, drawings, reports, and customer data are considered critical assets. These assets are the ones that will be given priority in risk management and control selection. The information contained in these assets is considered Confidential and the Confidentiality, Integrity of the information, Accessibility of Authorized Managers and Business Continuity are ensured.

7- INFORMATION SECURITY POLICIES, PROCEDURES AND GUIDES

ISMS Policy addresses many policies, procedures, instructions and guides published by our company within the framework of selected controls and risk management objectives. General information security rules are defined in this document published by information systems. Necessary precautions have been taken to ensure that every employee complies with the rules specified in this document.

The functioning of the system is explained in procedures and plans such as information backup, information security breach response, internal audit, control of documents and records, user identification, business continuity plan, emergency action plan, risk treatment plan. Relevant employees act in accordance with these procedures and plans defined and published by the management. All employees have undertaken to comply with corporate policies by signing confidentiality agreements defined and published by our company. The commitment and the rules are different documents. Personnel Confidentiality Agreement (Commitment) is a document signed by every hired employee (all permanent or contracted personnel, whether they use a PC or not).

8- INFORMATION SECURITY TRAINING AND COMPETENCE

The structure of our company, the processes it serves are defined, and the service qualification criteria, duties, powers and responsibilities for the personnel to be employed in the relevant processes are defined. Personnel employment is carried out in accordance with the provisions of the Human Resources Procedure.

Information security awareness trainings were organized for all our Company employees. The management taught all employees about the requirements, objectives, rules and sanctions of the information security management system, and awareness was provided. Information security training was provided to all new employees within the scope of compliance training.

Information security management system installation and risk management training was provided to ISMS Commission members.

The management allocates the necessary resources to raise awareness and train the ISMS unit and employees on information security.

9- CONTROL OF DOCUMENTS AND RECORDS

A Documented Document and Records Control Procedure has been prepared to fulfill the purposes of preparing ISMS-related documents, approving them before publication, tracking changes and revisions, and making the eastern version accessible at necessary points. Control of documents is carried out in accordance with this procedure.

The above procedure has been prepared and implemented in order to ensure that the records are controlled, stored, backed up and retrieved when necessary.

10- INFORMATION SECURITY INTERNAL AUDITS

Regular internal audits are planned to determine the compliance of the established information security management system with the standard and defined policies and procedures. The Internal Audit Procedure has been defined on how internal audits will be carried out, and regular internal audits are carried out in accordance with this procedure and non-conformities in the system are detected.

11- CONTINUOUS IMPROVEMENT AND CORRECTIVE ACTIONS

Corrective Action Procedure and BG Violation Incident Management Procedure have been prepared and implemented regarding how to eliminate the non-conformities that arise during internal audits, violations or employees' own observations, and how to fix potential non-conformities that arise in the detection of situations that do not comply with our standards, policies, procedures and rules. All personnel are responsible for participating in corrective actions.

INFORMATION SECURITY POLICY WEB VERSION

Our company's ISMS policy; It has been determined to include the responsibilities of the services provided by our business, the commitment to comply with the legislative requirements and the continuous improvement of its effectiveness, and to create a framework for the establishment and review of ISMS targets.

Our company ensures that our ISMS policy is communicated and understood and reviews it in management review for ongoing compliance.

Depending on our company's mission and vision, our primary field of work is to provide information technology services to our contracted customers.

OUR PRODUCTION AND SERVICES;

- Meeting the expectations of our customers and the institutions / organizations we serve within the scope of the contract at a high technology level, providing software and software development solutions at an advanced level, increasing their information technology capabilities, helping them achieve their activity / process / performance targets by informing them of technological developments are carried out within the scope and boundaries of ISMS.

- Accepting that all kinds of confidential / commercial / private information processed in all information technology systems we serve within the scope and boundaries of ISMS is the privacy of the customer of the institution / organization we serve, we accept that this information can be transferred anywhere / person / institution / organization without the knowledge / approval of the customer. Unobtainability has been ensured by adhering to the Integrity / Availability conditions.

- BGYS Our company's ISMS policy, provided that it remains within the scope and boundaries of the ISMS, complies with legal and regulatory requirements and takes into account the obligations or dependencies arising from contracts or third parties.

Our company declares that it will prove its commitment to the installation, implementation, operation, monitoring, review, maintenance and improvement of the Information Security Management System (ISMS) within the framework stated above by performing the following:

- ISMS objectives have been defined and plans have been made
- Risk analysis has been carried out, risk assessments and risk criteria have been put forward depending on the analysis results, and it provides risk management within this framework.
- Defined and ensured the importance of meeting information security objectives and compliance with information security policies, responsibilities to the law and the need for continuous improvement.
- Provided sufficient resources (financial, human resources, equipment, software, security, consultancy, training, etc.) to establish, implement, operate, monitor, review, maintain and improve the ISMS. provided sufficient resources (financial, human resources, equipment, software, security, consultancy, training, etc.) to implement, maintain and improve.
- Organizes and manages the necessary studies to determine risk acceptance criteria and acceptable risk levels.
- It will review the ISMS Policy at least once a year and make adjustments when deemed necessary and announce it to the relevant parties.