## 1. PURPOSE

This policy has been prepared to define the framework of information security requirements that employees and other relevant parties within YESPAN must comply with, by ensuring the confidentiality, integrity, and accessibility of information assets used within the organization only by authorized persons.

## 2. SCOPE

It covers all information systems involved in YESPAN's product delivery process, including IT resources, physical information assets, IT networks and infrastructure, application software, database systems, all platforms and processes where information is processed, as well as all stakeholders, including personnel and suppliers involved in these processes.

## 3. DEFINITIONS AND ABREVIVIATIONS

 **Information Security:** All measures taken to ensure the secure and reliable use of information and information processing facilities, to maintain their confidentiality and integrity, and to detect unauthorized access to information.
 **Information Security Incident:** Any event that compromises or has the potential to compromise the secure and reliable use of information and information processing facilities, including breaches of confidentiality, integrity, or unauthorized access.
 **Information Security Management System (ISMS):** A systematic, rule-based, planned, manageable, sustainable, and documented set of activities, approved by top management and based on international security standards, aimed at ensuring the confidentiality, integrity, and availability of information.
 **Top Management:** Executives who have the authority to make decisions and allocate resources on behalf of the organization.
 **CSIRT (Computer Security Incident Response Team):** The team responsible for responding to cybersecurity incidents.

## 4. INFORMATION SECURITY ORGANISATION

4.1 An Information Security Committee has been established to serve as the highest decision-making body within YESPAN on matters related to information security and cyber incident response, to support the activities carried out by the Information Security Officer and the organizational CSIRT, to monitor information security-related activities, and to carry out the necessary actions.

4.2 Cem Yıldırım has been appointed as the Information Systems Coordinator to coordinate the activities of the Information Security Committee and to chair its meetings.

4.3 Personnel have been appointed as members of the Information Security Committee, representing relevant units, to provide the necessary support in areas related to information security, including human resources, physical and environmental security, legal affairs, and information systems.

4.4 Information security activities within YESPAN are carried out in accordance with the procedures and principles set out below.

## 5. POLICY STATEMENT

5.1 The YESPAN Information Security Management System (ISMS) Policy is based on the Information Security Policies Directive and the Information Security Policies Guideline, and provides the operational and managerial framework to ensure the confidentiality, integrity, and availability of corporate information assets.

5.2 All personnel are responsible for carrying out their activities in compliance with the applicable legislation specified under the compliance section, and in accordance with the information security policies determined by top management, primarily this policy.

5.3 All personnel are responsible for being aware of the ISMS policies published at www.yespan.com and for implementing their requirements.

5.4 All personnel are responsible for reporting any information security incident to the ISMS Team, either in written or verbal form, upon becoming aware of it.

5.5 All personnel are required to comply with the rules established within the scope of physical security measures (such as entry and exit points, office rooms, product delivery areas, warehouse security, and the use of personnel identification cards, etc.).

5.6 External parties (including any suppliers requiring access) seeking to access IT infrastructure and services (such as server access, database access, etc.) must strictly comply with the organization's access procedures. Any unauthorized access attempts shall be considered an information security incident.

5.7 Within the scope of the information security policy, confidentiality agreements are signed with all stakeholders and relevant parties.

5.8 In the event of a violation of the Information Security Management System (ISMS) Policy, the relevant provisions of the Information Security Disciplinary Procedure shall be applied to the personnel responsible for the violation.

5.9 ISMS management representatives are responsible for updating and reviewing the information security policy document. Policies and procedures shall be reviewed at least once a year, revised based on risk assessments, and approved by top management. The updated version shall be published in a manner accessible to all users.

5.10 User devices used to access YESPAN's information assets are subject to security controls.

## 6. CONTINUOUS IMPROVEMENT

Continuous Improvement Commitment: We are committed to continuously improving the performance and effectiveness of the Information Security Management System (ISMS).

Management Review: We commit to participating in periodic “Management Review Meetings” and updating action plans in order to continuously improve the processes and activities used for the implementation of the ISMS.

Risk Management: We commit to continuously reviewing and enhancing ISMS risk treatment options and controls in line with risk assessment results and changes in business processes.

Objectives and Performance: We commit to continuously improving information security objectives, performance indicators, and the overall functioning of the ISMS through periodic reviews within annual plans to ensure a more secure structure.

Training and Awareness: In order to adapt to technological developments and the evolving threat landscape, we continuously update and improve personnel awareness activities within the scope of the ISMS.

## 7. COMPLIANCE WITH APPLICABLE LEGISLATION

YESPAN commits to full compliance with all applicable national and international legislation, regulations, and standards in all activities carried out within the scope of the Information Security Management System (ISMS). Within this commitment:

1. **Monitoring of Legislation:** YESPAN regularly monitors and updates all relevant laws, regulations, standards, and contractual requirements.
2. **Compliance Implementation:** Identified legal and regulatory requirements are integrated into ISMS processes and implemented.
3. **Employee Responsibility:** All employees are responsible for being aware of and complying with the legal requirements relevant to their roles.
4. **Audit and Improvement:** The level of compliance is regularly audited, and continuous improvement activities are carried out.

This clause reflects YESPAN’s commitment to fulfilling its legal and regulatory obligations in information security management.