1. Scope

This policy covers the definition of the roles and responsibilities required for the operation of information security processes, the establishment of processes for managing risks related to information systems, and the establishment and oversight of controls.

2. Purpose

The purpose is to define the requirements necessary to ensure the confidentiality, integrity and availability of the Company's information systems and information assets, and to protect, maintain and manage the confidentiality, integrity and availability of information and all supporting business systems, processes and applications. This means ensuring that information remains in authorized hands, that information is complete, accurate and available, and that information and systems are ready for use when required.

The Information Security Policy has been prepared by taking into account the Communiqué on Information Systems Management (VII-128.9) issued by the Capital Markets Board for publicly traded companies, the TS EN ISO 27001 Standard, the Personal Data Protection Law and other regulations.

The Company ensures the establishment and oversight of the controls required for the operation and continuity of the Information Security Management System processes through sub-policies, procedures and instructions linked to this policy.

The Company has adopted the fulfilment of the following matters in particular:

− Managing information assets, determining the security values, needs and risks of such assets, and developing and implementing controls for security risks.

− Defining the framework to be used by the methods for determining information assets, their values, security needs, vulnerabilities, threats to assets and the frequency of such threats.

− Defining a framework for assessing the confidentiality, integrity and availability impacts of threats on assets.

− Setting out the working principles for risk treatment.

− Continuously monitoring risks by reviewing technological expectations within the scope of the services provided.

− Meeting information security requirements arising from national or international regulations to which the Company is subject, compliance with legal and relevant regulatory requirements, obligations arising from agreements, and corporate responsibilities towards internal and external stakeholders.

− Reducing the impact of information security threats on service continuity and contributing to continuity.

− Having the capability to respond rapidly to information security incidents that may occur and to minimize their impact.

− Maintaining and improving the level of information security over time through a cost-effective control infrastructure.

− Enhancing corporate reputation and protecting it from negative impacts arising from information security.

− Ensuring the continuity of the Information Security Management System.

− Supporting all activities aimed at continuously improving the Information Security Management System.

3. Responsible Parties

A. Board of Directors

The information security policy is prepared by senior management and approved by the Board of Directors. The Board of Directors is responsible for establishing effective and adequate controls over information systems within the scope of the information security policy. The Board of Directors authorizes the "Senior Management" responsible for overseeing the policy. The authorities and responsibilities to be assigned shall be consistent with the principle of segregation of duties.

B. Senior Management

Senior Management shall be responsible for establishing and maintaining the general management framework related to Information Security, and for ensuring that this policy is continuously reviewed so that it remains up to date and continues to reflect

Senior Management: Refers to the person or group designated by the Board of Directors, or, where no designation is made by the Board of Directors, the Company's highest-ranking officer.

the business requirements of the Company and its subsidiaries, as well as changes in the risk environment or threats faced by their information and information systems. The Board of Directors has authorized Senior Management, consisting of the Deputy General Manager for Corporate Governance, to approve all standards, procedures and instructions required to be prepared within the scope of the policy.

The implementation of the information security policy is overseen by Senior Management. Senior Management demonstrates the necessary commitment to bringing information security measures to an appropriate level and allocates sufficient resources for the activities to be carried out for this purpose. In order to ensure that security risks arising from information systems are managed at an adequate level, Senior Management ensures the development, operation and currency of controls relating to measures that will ensure the confidentiality, integrity and availability of information systems and the data processed, transmitted and stored on them, and defines the necessary managerial responsibilities.

The oversight and responsibilities of Senior Management are as follows:

− Reviewing and approving information security policies and all responsibilities annually,

− Performing risk management, including the identification of potential risks related to information systems and processes together with their impacts, and the definition of activities to mitigate such risks within this framework,

− Monitoring incidents related to information security breaches and evaluating them annually,

− Carrying out activities and providing training to increase information security awareness among all employees.

− Ensuring that the processes and procedures established for the management of risks related to information systems are embedded in the organizational and managerial structure in a way that functions in practice, and carrying out oversight and follow-up regarding their effectiveness.

− Appointing an Information Systems Security Officer who is responsible for fulfilling and monitoring the requirements of processes and procedures related to information systems security, who reports to senior management on information systems security risks and the management of such risks, and who has sufficient technical knowledge and experience.

− Preparing a business continuity plan to ensure the continuity of all critical business processes according to risk priorities. The plan identifies the acceptable interruption periods and maximum acceptable data loss for critical business processes.

C. Information Systems Security Officer

The Information Systems Security Officer, consisting of the Information Security Management Team (ISMS Team), is responsible for fulfilling and monitoring the requirements of processes and procedures related to information systems security, and is a person who reports to senior management on information systems security risks and the management of such risks and who has sufficient technical knowledge and experience. In general, the Information Systems Security Officer provides guidance in handling information security incidents, ensures that the policy is supported by detailed standards, procedures and processes, and ensures that these are available for use when needed. The Information Systems Security Officer is also responsible for ensuring that the requirements of this policy are communicated to all employees (permanent or temporary) and all contractor personnel. The functional ownership of this policy, all standards, other supporting documents and training activities shall be carried out by the Information Systems Security Officer, and this role shall also serve as a source of advice and guidance regarding the implementation of the policy across the Company.

D. Other Stakeholders

All employees are obliged to comply with all policies and procedures published under the Information Security Management System category, to report actual or potential security breaches and vulnerabilities, and to carry out all activities requested by the Company. Regardless of their position or duties, Company employees are responsible for performing their work in a manner that safeguards the protection of information within the Company. Information Security Policies are valid and mandatory for all personnel who use information or business systems, whether full-time or part-time, permanent or contracted, regardless of geographic location or business unit. In this context, Asset and Process Owners are responsible for:

− Complying with the Information Security Policy and procedures communicated to them.

− Ensuring compliance with Information Security documents in the documents they prepare for the management of their own processes and systems, such as process documents, workflows, instructions, guides and forms.

Senior Management: Refers to the person or group designated by the Board of Directors, or, where no designation is made by the Board of Directors, the Company's highest-ranking officer.

− Reporting any non-compliance with Information Security policies and/or procedures or any information security breach incidents to info@kafein.com.tr.

− Not engaging in activities that may adversely affect the operation of information systems or jeopardize information security.

− Communicating update/improvement requests regarding Information Security documents to the Information Systems Security Officer.

− Requesting access to information and corporate resources to the extent required by business needs.

− Determining access rights to the owned asset and Personal Data, and determining who may access them with which privileges at administrator and user levels.

− Monitoring the asset inventory and ensuring that it is kept up to date,

− Ensuring the classification, updating and review of the assets they own, including Personal Data.

The principles of the Information Security Policy shall be implemented in parallel with the rules of the Company Human Resources Personnel Regulation. Employees are also responsible for being aware of the Information Security Policy and complying with these principles.

Any Company employee may request the Information Systems Security Officer to amend the policies in order to improve the Information Security Policies and better reflect the controls needed by the Company. Such requests are handled and evaluated by the Information Systems Security Officer.

Third Parties

The information security rules to be followed by third parties providing goods and services to the Company and their employees are determined by the relevant agreements and security protocols. These include, at a minimum, the following:

− Acting in accordance with the Company Policies and Procedures governing relations with third parties, particularly the information security rules communicated through agreements or protocols.

− Not sharing Company information and assets with others without the Company's approval and permission.

− Using the identities provided to them by the Company in accordance with agreements and instructions.

− Not copying any data or software on the Company's devices, not making audio recordings, taking photographs or videos of the environment, or engaging in any sharing/actions that could endanger data security or the Company's image, without the Company's approval and permission.

− Performing system accesses at Company locations under the supervision of the Information Technology teams.

All persons who are not classified as Company personnel but who need access to Company information, such as third-party service providers and their affiliated support personnel, must adhere to the general principles of this policy and to the other security responsibilities and obligations with which they are required to comply.

4. Audit and Control

In order for Information Security Policies to reflect the current risks faced by the Company's information assets, "Risk Analysis and Internal Audits" relating to information systems are carried out at least once a year in parallel with asset and risk updates. In order to keep new risks and changes in risks under control, the Information Security Policies are updated by making the necessary additions or amendments. The Company is subject to a "Penetration Test" at least once a year by real or legal persons who have no duty in relation to the fulfilment of information security requirements and who hold a national or international certificate in penetration testing. The procedures and principles regarding penetration testing are based on the conditions set out in the annex to the CMB Communiqué on Information Systems Management.

Kafein meets the requirements of the "TS EN ISO 27001" standard and is subject to audits by TÜRKAK-accredited organizations. "Recertification" is performed once every three years. During the entire cycle, "Surveillance Audits" are carried out every year.

The Information Systems Security Officer is responsible for periodically auditing compliance with all published policies and procedures and relevant standards, primarily the Information Security Policy, and reporting to Senior Management. Senior

Senior Management: Refers to the person or group designated by the Board of Directors, or, where no designation is made by the Board of Directors, the Company's highest-ranking officer.

Management oversees the implementation of the policy, appoints responsible persons, and approves all standards, procedures and instructions required to be prepared.

The effectiveness, adequacy and suitability of information systems controls and the activities intended to mitigate the relevant risk or risks are continuously monitored and evaluated.

Significant control deficiencies identified as a result of the evaluation are reported to Senior Management and the necessary measures are ensured to be taken.

Violations of the Information Security Policy may cause the Company to suffer damage as a result of the failure to implement the controls required against risks, and may also give rise to criminal liability under the new Turkish Criminal Code and liability to compensate material damages. Therefore, such violation also constitutes a violation of the Company Personnel Regulation and may result in disciplinary action. Information Security Policy violations identified through oversight, audit or notification may result in the application of internal disciplinary penalties, termination of employment, and even the initiation of judicial and criminal legal proceedings.

5. Entry into Force

This Information Security Policy has entered into force by resolution of the Board of Directors. Where any amendment to the Information Security Policy is required, the amended provisions shall become effective after approval by the Board of Directors. The approved information security policy is announced to personnel.

Company Board of Directors

Senior Management: Refers to the person or group designated by the Board of Directors, or, where no designation is made by the Board of Directors, the Company's highest-ranking officer.