BİM BİRLEŞİK MAĞAZALAR A.Ş.
INFORMATION SECURITY POLICY

The essential aspects of BİM's Information Security Policy are given below.

The Information Security Policy has been prepared by taking into account the VII-128.9 Information Systems Management Communiqué (Communiqué) which was put into effect by the Capital Markets Board for publicly traded companies, the Law on the Protection of Personal Data and other regulations on the subject.

1. PURPOSE

The purpose of BİM in managing information security is to ensure that the information is evaluated within the scope of confidentiality, integrity and accessibility, and that it is protected from all threats that may come from inside and/or outside, intentionally or accidentally, and that the activities are carried out effectively, accurately, quickly and securely.

The purpose of the information security policy is to inform all relevant parties about BİM information security requirements and to form the basis of written rules about information security.

2. SCOPE

BİM Information Security Management System covers all assets and technology categories of BİM.

3. RESPONSIBILITY

Board of Directors

The adequacy and the efficiency of the controls determined by this policy and the procedures to be prepared in line with it are under the responsibility of the Board of Directors.

Senior Management

The responsibility for the implementation and enforcement of this policy is the Senior Management level to which the unit (s) responsible for the management of information systems is affiliated. The relevant senior management provides the necessary resources for the implementation of the information security policy.

Information Technologies Directorate

BİM Information Technologies Directorate is responsible for defining the information systems risk management processes, controls and supervision mechanisms.

Unit Managers

Unit managers are responsible for implementing the Information Security Policy and ensuring the commitment of their employees to the principles.

Each BİM employee

Each BİM employee is responsible for knowing the Information Security Policy and rules; acting in accordance with these rules and principles, reporting security violations.

Contracted Suppliers/Business Partners

Contracted suppliers and/or business partners are responsible for complying with this policy and the principles, procedures and instructions put into effect by it.

4. INFORMATION SECURITY OBJECTIVES

By fulfilling the requirements of the Information Security Management System, the objectives of information security are to increase the awareness of the employees about information security, to apply technical security controls and to ensure that the basic and supportive business activities of the organization continue with the least interruption, to protect the security, reliability, and the image of the company through mitigating risks.

5. PRINCIPLES

All kinds of information can only be accessed within the predefined authority by service users, service providers and third parties.

Necessary operations are carried out to ensure the confidentiality, integrity and continuous accessibility of information.

Regardless of whether it belongs to service users and providers or third parties, the confidentiality of the information produced and/or used is guaranteed in all cases.

Proper usage is controlled in accordance with the principles set forth in the **"Usage Procedure in Compliance with Security Standards"** and the information is protected against unauthorized access.

Portable Computer usage will be controlled in accordance with the principles set forth in the **"Bim Portable Computer Usage Procedure"** and the information will be protected against unauthorized access.

The requirements determined by laws, regulations, circulars and contracts will be met. Working in harmony with them will also be provided.

Business continuity management will be implemented in order to protect critical business processes from the effects of major disasters and operational errors.

Trainings that will increase the information security awareness of the personnel and encourage them to contribute to the functioning of the system will be regularly given to the existing and newly recruited employees.

All unit managers will be primarily responsible for the implementation of these principles and will ensure that their personnel work in accordance with the principles.

6. REVIEW

9.1. Information Security Policy is reviewed to consider organizational changes, business conditions, legal and technical regulations, etc. in order to comply with the actual requirements.

9.2. These principles are regularly reviewed at least once a year and the changes made are submitted to the approval of the Board of Directors. Changes to the procedures can be implemented with the approval of senior management.