BATI ANADOLU GROUP OF COMPANIES INFORMATION SECURITY POLICY

Batıçim Batı Anadolu Çimento Sanayii A.Ş. and its subsidiaries over which it has direct and indirect control (“**Batı Anadolu Group of Companies**”) within T.S. ISO 27001 Information Security Management System with of data security, integrity And accessibility will provide to precautions related control of infrastructure To supervise the development and regular updating of Information Systems technical support to all units using the infrastructure, third party users and Information Systems. It is essential to ensure the security of service, software and hardware providers that provide support taking activities continues.

Each user is trained on Information Security at the beginning of his or her employment and is informed about their responsibilities and duties. Knows the established systems. Periodically, Information Systems Security awareness training is provided to departments is given.

• Personal knowledge your privacy to be protected to ensure for the purpose of customer and employee of your information your privacy protects.

• Infrastructure and infrastructure that will protect the integrity of information and guarantee its continuous accessibility controls brings it to life.

• Ensuring the minimum authorization principle required for authorization of users and your powers organised aspect control enables it to be done.

• Users' access rights to the system are granted at the end of each month; It checks the "Employee and User Accounts report" for Oracle, checks the report received from the system for AD and the employee report received from Oracle by matching them on Excel, and terminates the accounts and authorizations of the people who have left the job, if any.

• Created “BTA-BSB-TB-001 - POSITION BASED STANDARD RESPONSIBILITY TABLE" in line with per year two times all responsibility appointments control provides.

• It establishes network security against threats that may come from external networks and in this context, it is updated once a year. to be Penetration test for is applied.

• Used encryption of the keys its reliability provides.

• A complex password policy is applied to the passwords that employees will use to connect to the system, and they are forced to change their passwords every 90 days. Senior management and blue collar employees are excluded from the scope of this policy.

• Necessary security in all relevant areas to control access to information and prevent unauthorized access controls brings it to life.

• Information Security with relating to all legal to legislation rapport provides.

• Identifies risks to information assets and manages risks in a systematic manner.

• Ensures that the organization's core and supporting business activities continue with minimum interruption.

• Performs and records restore tests from backup once a year for Oracle Business Management System and once every six months for servers on virtual environment.

• It quickly intervenes in information security incidents that may occur and has the competence to minimize the impact of the incident.

• All vulnerabilities in Information Security that actually exist or arouse suspicion are reported to the BGS Team by all employees who detect or suspect them and are investigated by the BGS Team.

• It is ensured that necessary actions are taken by continuously identifying risks regarding Information Security.

• Within the scope of the Information Security Management System, the above items and other necessary policies are instructed and implemented in our organization.

We undertake to carry out the necessary work for the establishment, execution and continuous improvement of the Information Security Management System.