ELECTRONIC COMMUNICATION AND ELECTRONIC DATA ABOUT THE INSPECTION REGULATIONS

KVKK_Y4 VERSION 1.00

1. PURPOSE AND SCOPE

1.1. The purpose of this Regulation is to determine the procedures and principles regarding the conditions and timing of the Company's monitoring of electronic communications, and the provisions of this Regulation apply to personnel and third parties authorized to access and/or use the Company's electronic communication facilities.

2. MONITORING OF ELECTRONIC COMMUNICATIONS

2.1. For the purposes of this Regulation, electronic communication generally refers to all types of electronic messages, including telephone calls, fax messages, e-mails, instant messages, SMS or other short messages, tweets, wikis, blogs, and web content published on messaging platforms. The Company has no responsibility or duty to generally monitor the content of electronic communications of its personnel or visitors due to the nature of its operations. Furthermore, the Company does not routinely conduct general screening of electronic communications through random sampling or human intervention. However, automated computer-assisted screening of e-mail traffic is carried out to a limited extent to prevent unsolicited bulk e-mails (commonly referred to as "spam") and potentially harmful message content (computer viruses, financial fraud attempts, etc.).

2.2.5.4. All users acknowledge that by using the electronic communication systems provided by the Company, the Company makes no representations regarding the confidentiality of any messages or data stored on or sent through said systems; that the Company reserves its rights as stated in this document; and that the use of said systems is limited to purposes approved by the Company, and that they have been notified of this. The use of the Company's electronic communication systems in relation to Company activities and non-essential personal use is not a right, but a privilege granted to its employees and authorized third parties.

Therefore, the Company may, at any time and without prior notice, completely or partially block access to all or part of its electronic communication and IT systems (for all users or some users). Users of the Company's electronic communication and computer systems are obliged to comply with the Company's Regulation on the Procedures and Principles Regarding the Use of Information and Communication Technologies and Section 11.9 "Acceptable Use Conditions of IT Resources (Acceptable Use Policy)" of the Information Security Policy, and by using said systems, they acknowledge that they have accepted and will comply with the Acceptable Use Policy, that they have been notified of this, and that they have given their consent to the Company's implementation of the Acceptable Use Policy. Users also agree to comply with the relevant legislation and to refrain from any conduct that would obligate the Company. The Company may, at any time and without prior notice, change the Regulation on the Procedures and Principles Regarding the Appropriate Use of the Internet and Electronic Communication Tools and other conditions relating to the use of computer systems.

We reserve the right to make changes and to take any action required or appropriate under the relevant legislation.

2.3. In accordance with Article 6 of Law No. 5651 on the Regulation of Publications Made on the Internet and Combating Crimes Committed Through Such Publications, titled "Obligations of the Access Provider," the Company shall take the necessary measures to store electronic communication traffic information received or sent by the Company, limited to the purposes listed in the law, and to ensure the accuracy, integrity, and confidentiality of this information. These measures include, but are not limited to, monitoring whether the information is being used for criminal or unauthorized purposes, conducting audits and interventions to protect the system against threats such as viruses, hacking, and denial-of-service attacks, and ensuring the compliance of IT operations with the Company's policies and directives.

2.4. Monitoring of electronic communications will primarily be carried out with the consent of the relevant person. However, the Company reserves the right to conduct monitoring ex officio to achieve its legitimate purposes in the following cases:

2.4.1. Keeping records of transactions and other communications where it is necessary or desirable to know certain elements of the communication between relevant parties in order to ensure the security of financial and economic business and transactions;

2.4.2. To confirm compliance with regulations and practices concerning the Company, such as checking whether the Company's administrative regulations and internal guidelines and codes of conduct are being implemented;

2.4.3. To define or demonstrate the standards that must be achieved by persons using the Company's electronic information systems for purposes such as quality control or personnel training;

2.4.4. Monitoring or recording to prevent or detect criminal acts, for example, corruption, misuse of computer systems, or other illegal activities.

2.4.5. To prevent or detect unauthorized use of electronic information and communication systems, for example, to prevent employees from violating Company regulations mentioned in Section 11: "Terms of Use of IT Resources (Acceptable Use Policy)" of the Information Security Policy;

2.4.6. To ensure the effective operation of the system by detecting and removing viruses, controlling and stopping other system threats such as hacking or denial-of-service attacks; and by creating network flows and email logs;

2.5. Individuals using the Company's electronic communication systems should be aware that Information and Communication Technologies Systems and Network Administrators periodically monitor transmissions or observe transaction information to ensure the proper functioning of the Company's IT services. In such cases, the personnel concerned may inadvertently access electronic information.

They may be aware of the content of the communication. Unless otherwise specified in this Regulation or relevant legislation, it is prohibited for the aforementioned officers to knowingly review the content of the transaction information of Company employees or to otherwise use what they have seen, heard, or read. However, if a violation of Company policies and administrative regulations or legal provisions is detected, the matter must be reported to the Company's senior authorities.

3. ANALYSIS OF ELECTRONIC DATA

3.1. The Company may occasionally need to review corporate emails stored on network-connected or independent storage devices, documents and files located on local, main, or group drives, and data relating to access records to the Company's systems or buildings. In addition, employees and visitors connecting to the Company network with their individual devices are deemed to have consented to the monitoring of their data for the purposes limited to those specified in Section 6 of the Company's Information Security Policy, titled "Monitoring of Electronic Communications." These audits are limited to ensuring data security and will be conducted in accordance with the principles set forth in the Law No. 6698 on the Protection of Personal Data.

3.2. Under normal circumstances, the Company will obtain the user's consent before conducting any review of data held by or relating to individuals, such as email accounts, main drivers or local drivers, and access log records. However, the review will be conducted even if the user has not given permission in the following cases:

3.2.1. Where provided for by law;

3.2.2. If there is credible evidence beyond mere gossip or rumor, and there is strong suspicion that legal provisions or Company policies may have been violated;

3.2.3. In compelling circumstances and emergencies where failure to act would result in serious physical harm, significant loss or damage to property, loss of significant evidence of a violation of law or Company policies and regulations, or significant financial liabilities to the Company or its employees and/or directors;

3.2.4. Failure to take action may affect the administrative or financial functioning of the Company. if their ability to fulfill their responsibilities is likely to be severely impaired.

3.3. If the relevant user is located elsewhere than the Company's buildings and facilities, and the examination of data held by or relating to the user is necessary for commercial reasons, the relevant user's consent must be obtained first. If the user cannot be contacted, the relevant Department Head and the General Manager may grant written permission to conduct an audit of the computer or other devices allocated to the user for the purpose of conducting Company business. In this case, the necessary consent must be obtained.

The measures and reasons requiring inspections will be recorded in a report.

3.4. If it is necessary to review data held by a user or relating to individuals, as stated in section 3.2 above, without obtaining the consent of the data subject, the following rules shall apply:

3.4.1. Emergencies: The minimum requirements of the emergency situation may be examined, and the minimum measures necessary to remedy the situation may be taken immediately without permission; however, once the emergency situation has passed, appropriate permission must be sought without delay, and the situation must be recorded in accordance with paragraph 3.3;

3.4.2. In all other cases, no action will be taken without the written permission of the relevant Department Head and the General Manager.

3.4.3. Encrypted Data: If encrypted data is found during a system audit, the decryption key must be provided upon request.

3.4.4. The possession of data created by or relating to employees who are no longer employed by our Company belongs to the Company, subject to the provisions regarding legal destruction periods. It is not necessary to obtain the permission of the terminated employee to review such information. Permission to view the information must be obtained by following the procedure specified in section 3.3 above.

3.5. Once permission is granted, the data in the Company's systems will be processed as follows: will be discussed:

3.5.1. Company-related materials will be evaluated according to normal business practices. They will be kept or deleted as deemed necessary.

3.5.2. Personal data will not be examined unless there is a legitimate reason.

3.5.3. Company employees are responsible for deleting their personal data contained in electronic documents and emails before their employment is terminated.

3.6. Privacy: All audits conducted under this Regulation will be carried out with due regard for the right to privacy. Materials concerning individuals' private lives will be subject to the minimum scrutiny necessary for the purposes of the audit. Any confidential information encountered that is not relevant to the purpose of the search will not be disclosed to any party and will remain confidential. However, if any material is found during audits that is illegal or contrary to Company policies, the General Manager will be immediately informed and action will be taken in accordance with his instructions.