ELECTRONIC MESSAGING USAGE PROCEDURE AND REGULATIONS ON ITS PRINCIPLES

KVKK_Y5 VERSION 1.00

1. INTRODUCTION, OBJECTIVES AND DEFINITIONS

1.1. Electronic communication applications such as email and calendar are important communication tools for the Company and are used as an efficient tool for conducting a large part of the Company's business. This Regulation aims to determine the procedures and principles regarding the acceptable use of electronic communication applications used in the Company's activities, including economic activities, research, and administrative services. Furthermore, the security of these applications and the protection of personal data processed within these applications are explained in detail, along with the relevant rules and regulations.

1.2. Kardelen Paint and Chemical Industry Trade Limited Company uses Microsoft's Office 365 service, including the "Office" software used by its employees, as its electronic communication program. This Regulation sets out the guidelines to be followed regarding the use of electronic communication systems used within the Company, including but not limited to Outlook and Skype for Business.

1.3. In this Regulation, the term "message" means any written communication sent, received, or published using electronic communication software, including any attached documents, recordings, images, or other files.

2. SECURITY

2.1. Access to the content of all email accounts is subject to the reasonable grounds described in Section 11.9 "Acceptable Use Conditions of IT Resources (Acceptable Use Policy)" of the Company's Regulation on the Supervision of Electronic Communications and Electronic Data and Information Security Policy.

2.2. Email and calendars are not services with guaranteed security. For example, it is possible for unauthorized individuals to monitor the transmission of emails or calendar items, or to send fraudulent emails using a user's name. Therefore, users should not include any confidential or personal information in electronic messages unless the information is encrypted. Protecting the security of personal or sensitive data is a mandatory consideration when sharing information. The company and its employees have legal, ethical, and moral obligations to protect the security and confidentiality of special categories of data in the collection, processing, storage, and transfer of such data. Each piece of data deemed special should be protected with reasonable encryption methods. When transferring such data, it is necessary to consult the IT Support Team regarding the protection of confidentiality and privacy, and the general rules stipulated in the Data Transfer Security Policy must always be adhered to.

2.3. To improve collaboration among our employees, calendar items with subject lines can be set to be visible to other Company personnel by default. Therefore, all Company employees should refrain from placing any sensitive information (including personal data) in the subject line of calendar items.
Notes in a calendar entry, including attachments, are by default not visible to others. However, sensitive or personal data should still be avoided in calendar entries in accordance with the principles outlined in Section 1. Please review the relevant sections of our Company's Information Security Policy and Personal Data Protection Policy regarding Company sensitive data and special categories of personal data that must remain confidential. Also, please note that other personal information may be considered sensitive depending on the circumstances, such as the names of individuals attending meetings, types of permissions (hospital appointments, family emergencies, etc.). The subject lines of private calendar entries can be made invisible to others by selecting the "padlock" symbol to make them private.

2.4. Company corporate email accounts can be accessed from anywhere using the "Outlook Web Application" in any web browser . When using the "Outlook Web Application," the session times out after 1 hour if inactive to prevent unauthorized access to the account. After this period, the system prompts you to re-authenticate by entering your username and password.

2.5. Users should be careful when composing email communications and should bear in mind that the AutoComplete function may suggest an email address different from the intended one. If sensitive personal or company data, or special categories of personal data, are sent to an incorrect email address, the potential or actual data breach must be immediately reported to the relevant parties and recorded using the form included in the Regulation on Personal Data Breach Response Plan.

3. ARCHIVING, RETENTION PERIOD AND DELETION

3.1. All messages older than two years will be automatically moved to archive folders for new users. To search for/find emails older than two years, users will need to go to the "online archive" section. To change this setting, one of the following options can be selected using the "Assign Policy" option under the "Home" menu:
• Archiving (All email messages are stored in the default folders in Outlook (e.g. (Inbox and Sent Items) will be saved and will not be automatically archived.

• Archive emails older than 2 years.

3.2. Email messages are normally never deleted. Company corporate email users can choose from the following options: • Delete messages older than 5 years • Delete messages older than 10 years • Store all messages indefinitely

3.3. If any of the "delete" options mentioned above are selected, messages older than the time period selected by the user will be automatically deleted without further warning.

3.4. When an employee's employment with the Company is terminated, their account will be deactivated using a "soft delete" process, meaning it will be deactivated as of the date of departure. The email account will no longer be accessible. Six months after the date of departure, the accounts will be completely deleted, and after that, the mailbox will be completely cleaned 30 days later. Relevant employees may request to retain their Company username/email account for up to six months to ensure the continuity of Company operations. In this case, authorization will be granted upon request by the Department Heads and IT Manager.

3.5. There is a company policy that allows department managers to access employees' emails and files after their departure to ensure the continuity of company operations. Therefore, it is advisable for employees whose employment with the company is being terminated to delete all personal emails and files before leaving.

4. USE OF EMAIL ADDRESSES OTHER THAN THE COMPANY'S CORPORATE EMAIL ACCOUNT AND EMAIL FORWARDING

4.1. To ensure secure and reliable email communication, Company personnel are provided with corporate email addresses and a level of assurance is given regarding email delivery. This assurance does not apply if Company personnel use an external (non-Company) email account to conduct Company corporate communications and automatically forward official corporate emails to an external email account. Therefore, using an external email account for official Company business and transactions and automatic forwarding to external (non-Company) email accounts is prohibited.

4.2. Employees who believe they have a valid reason to forward their company's corporate email to an external email account should report this request to the IT Department.

5. OTHER MATTERS

5.1. The Company provides access to email systems solely for the purpose of conducting the Company's official business and transactions. Access to email for incidental and occasional personal use is prohibited.

This type of use is permissible as long as it does not interfere with the Company's operations, distract the employee (in terms of volume or frequency), or prevent others from accessing the network to conduct official Company business and transactions.

5.2. Union representatives who are company employees may use the e-mail system to communicate with union members and to conduct union business and activities.

5.3. It is advisable for all personnel to upload a new photo of themselves as an icon so that they can be recognized by other users in the Microsoft Office 365 environment. However, if an employee chooses not to share their photo publicly, they should not use a photo other than their actual reflection, or the Company logo should be set as the default.

5.4. All users, by using the electronic communication systems provided by the Company, acknowledge that 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 notice, block access to all or part of its electronic communication and IT systems (for all users or some users), in whole or in part. Users of the Company's electronic communication and computer systems are required to comply with the Company's Regulation on the Procedures and Principles Regarding the Appropriate Use of the Internet and Electronic Communication Tools and the Acceptable Use Conditions (Acceptable Use Policy). By using these systems, users acknowledge and agree to comply with the Acceptable Use Policy, that they have been notified of this, and that they consent to the Company's implementation of the Acceptable Use Policy. Users also agree to comply with relevant legislation and to refrain from any conduct that would place the Company's legal entity under obligation. The Company reserves the right to 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 at any time without prior notice, and to take any action required or appropriate to be taken in accordance with relevant legislation.

5.5. The Company shall protect the integrity of its internal electronic communication and computer systems and their users against unauthorized or improper use of said facilities and against violations of the Company's rules and policies.

To identify potential uses that could lead to violations, the Company reserves the right to restrict or block the use of any person without notice, and to search for, copy, remove, or modify any data, files, or system resources that could impair the intended use of computer systems or be used to violate the Company's rules or policies. The Company also reserves the right to conduct periodic checks of computer systems for their protection and any other rights. Examples of such checks include malware scanning of email messages processed on Company computers and servers.

5.6. The company is not responsible for any data loss or interference with files that may occur due to system malfunctions or other reasons related to the work it carries out to ensure the confidentiality and security of the systems in question.

5.7. Users may not authorize anyone to use their Company corporate accounts for any reason. The account holder is responsible for all use of the Company account. Users must take all reasonable precautions, including password protection and document protection, to prevent unauthorized use of their accounts. They should not share their passwords with anyone else and should change their passwords regularly. The account holder is responsible for any transaction made using a password belonging to a user account, even if the party performing the transaction is not the account holder themselves.

5.8. No electronic communication or IT system belonging to the company may be used irresponsibly or in a way that interferes with the work of others. This includes: transmitting or making available defamatory, offensive or harassing content, chain mail, unauthorized mass mailing or unsolicited advertising; intentionally, carelessly or negligently damaging a system, material or information that does not belong to the user; intentionally disrupting electronic communications or otherwise violating the privacy of others or accessing information that does not belong to or is not intended for the user; intentionally misusing system resources or causing others to misuse them; or downloading software or data to administrative systems from unreliable sources such as free software.

5.9. The company is in no way responsible for content that it does not provide itself through email and other communication systems. Users access content provided by others at their own risk, acknowledging that they may find it offensive, inappropriate, or objectionable. Email and IT systems are provided “AS IS” and “AS AVAILABLE”. The company assumes that third-party content is accurate, complete, and reliable.

The user absolves themselves of any liability whatsoever regarding this. The user is responsible for the information they hold or store in email systems.

5.10. The User acknowledges that (i) any attempt to hinder the operation of e-mail and other communication systems or their use by others; (ii) uploading content that overloads e-mail and other electronic communication systems; (iii) actions that endanger the general security of electronic communication systems and/or harm other users; (iv) using or attempting to use software that hinders or interferes with the operation of e-mail and other communication systems are absolutely prohibited.

In the event of any violation of this Regulation by another party, or any information regarding an error or bypass related to the security of e-mail and other electronic communication systems, it is mandatory to immediately report the incident to the IT Department.

5.12. Unauthorized or inappropriate use of the company's email and other electronic communication systems, including non-compliance with the provisions of this Regulation, constitutes a breach of company policy and requires disciplinary action with the approval of the General Manager.

6. REVIEW

The Deputy General Manager is responsible for reviewing and updating this document. Changes and updates are published with the approval of the General Directorate. The review takes place annually in June.