

COMMUNICATION TOOLS USAGE POLICY

DCS



Communication Tools Usage Policy

1 Purpose

The DCS Communication Tools Use Policy establishes the principles and rules governing the safe, effective, and responsible use of corporate email, telephone, corporate messaging and video conferencing platforms, and other corporate communication tools.

This Policy aims to ensure that communication tools are used in a manner that supports business processes and corporate objectives, that information assets are protected, that corporate communication standards are maintained, and that applicable legislation is complied with.

No provision of this Policy may conflict with the applicable laws to which the Company is subject.

2 Scope

This Policy applies to all users authorized by the Company to use corporate communication tools.

This Policy applies to all internal and external communication activities conducted using devices, systems, and communication tools provided by the Company.

The procedures and principles governing the implementation of this Policy shall be determined by the relevant instructions, procedures, and other Company regulations. Such regulations shall be prepared, implemented, and, where necessary, updated in compliance with this Policy.

3 Definitions

Communication Tools: means corporate email, telephone, video conferencing, corporate messaging platforms, and other digital communication tools provided by or approved for use by the Company for business purposes.

Confidential Information: means information assets belonging to the Company, customers, or other stakeholders that must be protected, including trade secrets, business strategies, financial data, personal data, and other information of a similar nature.

Personal Use: means the limited use of communication tools for personal purposes, provided that such use does not disrupt business processes or violate relevant Company policies and regulations.

4 Policy Statements

4.1 General Usage Principles

DCS communication tools are provided primarily for business use. Employees are required to use these tools safely, effectively, and responsibly in a manner that supports business processes and corporate objectives.

All written and verbal communications conducted through DCS communication tools shall adhere to the principles of professionalism, respect, business ethics, confidentiality, and corporate communication.

The procedures and principles concerning internal and external communication methods, as well as the authorities and responsibilities of the persons and units within this scope, shall be determined under the Communication Procedure and relevant Company regulations.

4.2 Email and Instant Messaging

- The procedures and principles governing email use are set out in the Email Use and Management Instruction.
- Employees are required to use only corporate email addresses assigned by the Company and approved communication tools in business processes.
- Email and instant messaging tools should be used primarily for information sharing and communication in connection with business activities.

4.3 Telephone and Video Conferencing

- Employees shall act in accordance with the principles of confidentiality, information security, and professional communication when conducting telephone and video conference calls. Particular care shall be taken to prevent confidential and sensitive information from being overheard by unauthorized persons, especially during calls conducted in public or shared areas.
- Telephone calls and audio or video meetings may be recorded only in accordance with applicable legislation and relevant Company regulations and, where required, by informing participants and/or obtaining their explicit consent.

4.4 Internet and Social Media Use

- Internet access and communication tools provided by DCS should be used primarily to support business activities.
- Employees shall refrain from visiting websites that are unrelated to work, inappropriate, unlawful, or may pose an information security risk. Users are responsible for any consequences arising from the use of internet access in breach of this Policy and relevant Company regulations.
- DCS may, where it deems necessary for the purposes of information security, business continuity, and the fulfillment of legal obligations, restrict or block access to certain internet addresses or content. Where an access request is required, users shall submit their reasons to Information Technologies. Users may not disable the security controls in place or attempt to render them ineffective.
- Employees shall assess the accuracy and reliability of information obtained from the internet and shall not use unverified information in business processes.
- When using social media for business purposes, employees shall represent DCS professionally, take due care to protect confidential information, and act in accordance with the provisions of the **Social Media Code of Conduct** and **Public Communication Instruction**.
- The procedures and principles governing internet access, the Company network, VPN use, and the secure use of communication tools are set out in the **Acceptable Use of Assets Instruction**.

4.5 Security and Data Protection

- Employees are required to comply with the relevant Company policies and regulations concerning the secure use of communication tools and the protection of information assets and corporate data processed through such tools.
- Confidential and sensitive information shall be shared only for business purposes and in accordance with the classification and protection rules set out in the Asset Classification Guide.
- Unauthorized access attempts targeting communication tools or information assets, data breaches, suspicious emails, malware, and other information security incidents shall be reported to Information Technologies without delay.
- Content created, processed, or shared through artificial intelligence-assisted applications shall comply with the rules governing the protection of confidential information, personal data, and other sensitive information, as well as the provisions of the **Artificial Intelligence Use Policy**.
- The principles and obligations concerning information security, the protection of personal data, and the classification of information assets are set out in the **Information Security and Data Protection Policy**, the **Personal Data Protection and Processing Policy**, and the **Asset Classification Guide**.

4.6 Prohibited Activities

Communication tools provided by DCS shall not be used for the following purposes:

- Creating, sending, sharing, or disseminating content that is contrary to applicable legislation or Company policies and regulations.
- Creating, transmitting, or sharing inappropriate content involving insults, threats, harassment, discrimination, hate speech, obscenity, or similar conduct.
- Engaging in activities that may damage DCS's reputation, undermine corporate trust, or expose the Company to legal, financial, or administrative liability.

- Using communication tools provided by the Company for personal commercial activities, secondary employment, or purposes unrelated to the Company's activities.
- Creating, transmitting, or disseminating spam, phishing, malware, or other malicious content, or facilitating its dissemination.
- Sharing confidential information, personal data, or other sensitive information with unauthorized persons or platforms.
- Using artificial intelligence-assisted applications in a manner contrary to the provisions of the Artificial Intelligence Use Policy.

5 | Responsibilities

5.1 Employees

- Use communication tools provided by DCS in accordance with this Policy and relevant Company regulations.
- Comply with the obligations relating to the secure use of communication tools and report suspicious circumstances, information security incidents, or uses contrary to this Policy to their manager and/or Information Technologies without delay.
- Act in accordance with professional, ethical, and corporate communication principles in all communications.

5.2 Managers

- Support efforts to inform employees about this Policy and relevant Company regulations and to ensure their compliance therewith.
- Oversee the implementation of this Policy in communication processes within their areas of responsibility and ensure that corrective actions are taken where necessary.
- Assess identified non-compliance relating to the use of communication tools in coordination with the relevant units.

5.3 Information Technologies

- Ensure the secure, effective, and uninterrupted operation of communication tools and systems.
- Implement technical measures relating to information security, data protection, and the protection of personal data, and provide the necessary technical support.
- Carry out testing, monitoring, and other technical controls deemed necessary to support the secure use of communication tools.
- Coordinate the assessment of identified information security incidents and the implementation of the necessary technical interventions.

6 | Training and Awareness

- Training, information, and awareness activities shall be planned and conducted during the recruitment process and at periods deemed necessary in order to raise employees' awareness of this Policy and relevant Company regulations.
- Training and awareness activities shall cover the secure use of communication tools, information security, the protection of personal data, corporate communication principles, the secure use of artificial intelligence-assisted communication tools, and compliance with relevant Company regulations.

7 | Monitoring and Compliance

DCS may, within the framework of applicable legislation, monitor the use of communication tools, review related records, and access them where necessary for the purposes of ensuring information security, maintaining business continuity, fulfilling legal obligations, conducting internal review and disciplinary processes, and monitoring compliance with this Policy.

Communication tools provided by the Company are allocated for corporate purposes, and users acknowledge that they are aware that such tools may be monitored and audited under applicable legislation and Company policies and regulations and that their records may be reviewed where necessary.

Monitoring and audit activities shall be carried out with due regard to the protection of personal data, the right to privacy, and applicable legislation.

Assessments concerning the implementation of this Policy shall be reviewed regularly within the scope of internal control, information security, and compliance activities.

8 | **Non-Compliance with the Policy**

In the event of non-compliance with this Policy, disciplinary processes may be applied in accordance with the relevant Company regulations, taking into account the nature, impact, and consequences of the violation.

Where acts contrary to applicable legislation are identified, the necessary legal and administrative proceedings may be initiated against the relevant person or persons.

9 | **Reporting and Protection of Reporting Persons**

DCS provides the necessary mechanisms for employees, suppliers, and other stakeholders to report concerns regarding violations of this Policy confidentially and without fear of retaliation. Employees shall report any non-compliance or suspicious situation they encounter, irrespective of whether the person engaging in the conduct in question is a manager or any senior employee.

Reports may be submitted to the Ethics and Compliance Function at etik@dcscustoms.com.tr.

DCS grants its employees the right to make reports without disclosing their identity and treats anonymous reports with the same level of seriousness. Pursuant to the Reporting, Consultation and Prevention of Retaliation Policy, all reports are handled confidentially and with measures in place to protect the reporting employee from retaliation.

DCS undertakes to investigate all reports concerning violations of this Policy promptly and fairly. If a violation is substantiated, the Company shall take appropriate corrective measures and work to remedy any harm caused.

10 | **Review and Revision**

This Policy shall be reviewed at least once annually under the coordination of the Ethics and Compliance Function, Information Technologies, and Corporate Communications, in line with applicable legislation, technological developments, business processes, and corporate needs.

Where necessary, amendment or revision proposals shall be submitted to the Board of Directors for approval. Approved revisions shall enter into force upon publication through the document management system.

