COMMUNICATION TOOLS USAGE POLICY

DCS

Compliance Program

Communication Tools Usage Policy

1 Purpose

The DCS Communication Tools Usage Policy outlines the principles and rules for the appropriate and responsible use of communication tools provided by the company, including email, instant messaging, telephone, video conferencing, and other digital communication platforms.

This policy aims to ensure that these tools are used in a way that supports business objectives, protects company assets, and complies with legal and regulatory requirements.

No provision of this policy may conflict with applicable laws to which the company is subject.

2 Scope

This policy applies to all DCS employees, contractors, consultants, and other individuals who use DCS communication tools.

It covers all communication activities carried out using company-provided devices and systems, including both internal and external communications.

Business processes and all relevant procedures shall be prepared, implemented, and audited in accordance with this policy.

3 Definitions

Communication Tools: Includes email, instant messaging, telephone (including mobile phones), video conferencing, and other digital platforms provided by DCS for business use.

Confidential Information: Any information proprietary to DCS or its clients, including trade secrets, business strategies, financial data, and personal data.

Personal Use: The use of communication tools for non-business-related activities.

4 Policy Statements

4.1 General Usage Principles

DCS communication tools are primarily allocated for business use. Employees are responsible for using these tools in a responsible, appropriate, and mindful manner to support corporate activities and goals.

All written and verbal communications through DCS communication tools must adhere strictly to professionalism, respect, business ethics, and workplace appropriateness.

Rules concerning internal and external communication methods and the responsibilities and authorities of related individuals and departments are detailed in the Communication Procedure, Social Media Conduct Guidelines, and Public Communication Instruction documents published on the DCS intranet under the CRM – Quality & OHS module.

4.2 Email and Instant Messaging

- The use of email, instant messaging, and other digital communication tools is governed by the provisions of the "Internet, Email, Company Phone and Social Media Usage" clause in the Indefinite-Term Employment Contract.
- Employees are required to use only the corporate email addresses provided by the company in business processes.
- Email and messaging tools should primarily be used for information sharing and communication related to business activities.
- All messages should be clear, business-focused, and appropriate in content; they must not include elements inconsistent with corporate culture and the professional environment.

- Employees must refrain from sending offensive, discriminatory, harassing, or otherwise inappropriate content that could damage company values.
- Unrelated messages that unnecessarily occupy the recipient or disrupt workflow must be avoided.
- Users who receive spam or phishing emails must immediately notify the IT department. To raise awareness, DCS may conduct at least one phishing test annually.
- Confidential and sensitive information should only be shared for business purposes and under necessary conditions, using appropriate security measures (e.g., encryption). Methods of sharing information assets must comply with the guidelines defined in the Asset Classification Guide available in the CRM – Quality & OHS module on the DCS intranet.
- Employees are directly responsible for all communications made via corporate communication tools.

4.3 Telephone and Video Conferencing

- Employees must pay attention to confidentiality, especially during phone or video calls in public or shared spaces. Sensitive discussions must be held in private areas where the conversation cannot be overheard.
- Employees must comply with DCS guidance on recording calls or meetings and ensure all recordings are made legally and with the consent of all participants.

4.4 Internet and Social Media Use

- In the workplace, internet access is only permitted via the company's local network and infrastructure that enforces information security measures like firewalls. Except in mandatory cases, direct access via external modems, mobile data, wireless networks, or similar methods is strictly prohibited.
- Outside the workplace, company computers used for business purposes must access internal systems and resources via the DCS VPN.
- Internet access through DCS communication tools must be limited to activities supporting business functions. Employees must avoid visiting inappropriate or high-risk websites. Users are personally liable for the consequences of unauthorized or inappropriate use of internet services and content.
- When necessary, DCS has the authority to block specific websites or content for individual, group, or company-wide access. Users may request access to blocked content in writing to the IT department with a valid reason. Users are prohibited from bypassing such restrictions.
- All internet-acquired information must be treated as unverified unless validated through other means. Only verified content may be used for business purposes.
- Detailed rules regarding internet access, network use, VPN, and communication tools are outlined in the "Acceptable Use of Assets Instruction" published in the CRM – Quality & OHS module on the DCS intranet.
- Unless part of their job responsibilities, employees must not use DCS communication tools for personal social media activities during working hours.
- When using social media for work purposes, employees must represent DCS professionally and avoid disclosing confidential information.

4.5 Security and Data Protection

- Employees are responsible for securing the communication tools and data transmitted via these tools. Devices must be password-protected, encrypted communications should be used when necessary, and confidential information must not be transmitted through insecure channels.
- Confidential data must be sent according to the protection levels defined in the Asset Classification Guide.
- Any suspected security breaches, including unauthorized access to tools or data, must be reported to the IT department without delay.
- Principles and obligations regarding data security and protection are detailed in the Information Security and Data Protection Policy.

4.6 Prohibited Activities

Employees are strictly prohibited from using DCS communication tools for the following purposes:

- Sending illegal, offensive, or discriminatory content
- Engaging in activities that may harm DCS's reputation or expose the company to legal liability
- Conducting personal business or unrelated commercial activities, such as running a side business
- Distributing spam, phishing content, or other malicious material

5 Responsibilities

5.1 Employees

- Use DCS communication tools in compliance with this policy and report any misuse or security concerns to their manager or the IT team
- Ensure all communications are professional, secure, and aligned with DCS business goals

5.2 Managers

- Ensure their teams are aware of and comply with this policy
- Monitor communication tool use within their departments and address any issues or potential risks immediately

5.3 IT Team

- Ensure the secure, continuous, and efficient use of communication tools and systems; take necessary technical precautions within the scope of information security, data protection, and KVKK
- Conduct regular tests, audits, and monitoring to ensure policy compliance and address any security gaps or breaches

6 Training and Awareness

- Employees will receive training on the proper use of communication tools during onboarding and through regular refresher sessions.
- Training will cover best security practices, acceptable use, and the consequences of policy violations.

7 Monitoring and Compliance

DCS reserves the right to monitor communication tool usage to ensure compliance with this policy, protect company assets, and maintain operational efficiency. Monitoring may include reviewing emails, messages, call logs, and internet usage.

Employees should have no expectation of privacy when using DCS communication tools. All communications are subject to lawful monitoring and review.

This policy's assessment is part of regular compliance reporting.

8 Policy Violations

Failure to comply with this policy may result in disciplinary action, including warnings, termination of employment, or cancellation of contracts with third parties, depending on the severity of the situation.

In cases of serious violations—especially if illegal or harmful activities are carried out using DCS communication tools—legal action may be pursued against the responsible parties.

9 Reporting and Whistleblower Protection

DCS provides mechanisms for employees, suppliers, and other stakeholders to report concerns about violations of this policy confidentially and without fear of retaliation. Employees should report any wrongdoing or suspected issue—even if it involves their manager or another superior.

Reports may be submitted to the Ethics and Compliance Function via email at etik@dcscustoms.com.tr or in person.

DCS also allows anonymous reporting and treats such reports with equal seriousness. All reports are handled in accordance with the **Whistleblowing, Consultation, and Anti-Retaliation Policy,** with appropriate measures taken to protect the whistleblower's confidentiality and prevent retaliation.

DCS is committed to promptly and fairly investigating all reported policy violations. If a violation is confirmed, the company will take corrective action and work to remedy any resulting harm.

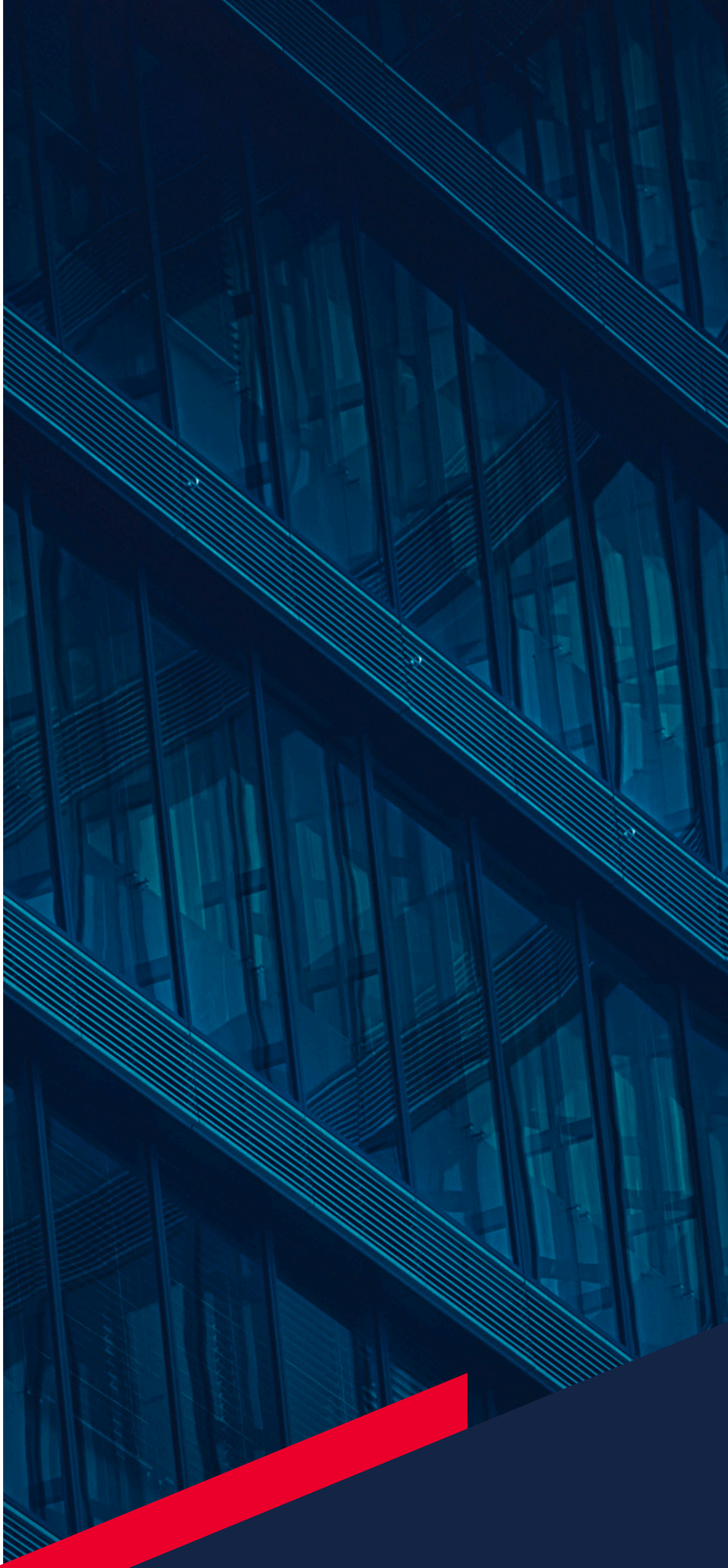
10 Review and Revision

This policy will be reviewed annually from its effective date for compliance with local and international laws. Reviews will be coordinated by the Ethics and Compliance Function and the IT Department to reflect changes in technology, legal requirements, and DCS business practices.

Other changes and revisions will be based on risk evaluations by the relevant departments and submitted to the Board of Directors with a justification report prepared by the Ethics and Compliance Function and the IT Department. Upon Board approval, the revised policy will be formally recorded via the document management system.

DCS

Compliance Program



www.dcscustoms.com.tr