PROTECTION OF PHYSICAL AND FINANCIAL ASSETS POLICY

DCS | Compliance Program

Protection of Physical and Financial Assets Policy

1 Purpose

The DCS Asset Protection Policy establishes the principles for protecting all physical and financial resources of DCS, particularly its information systems and information assets.

This policy ensures that all assets are used responsibly, properly maintained, and protected against theft, loss, misuse, or damage.

None of the provisions of this policy shall contradict any applicable laws to which the company is subject.

2 Scope

This policy applies to all employees, contractors, and other individuals who have access to or manage DCS's physical or financial assets.

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

3 Definitions

Information System: Includes all servers, clients, network infrastructure, data, and computer components owned or protected by the company. The use of information systems also includes internal and external services such as internet access and email.

Information Assets: Assets such as information systems, software licenses, service subscriptions, domain names, written documents, equipment, phones, portable computers, and stored data.

Physical Assets: Buildings, equipment, machinery, vehicles, furniture, computer hardware, and all other tangible resources owned, leased, or managed by DCS.

Financial Assets: Cash, bank accounts, securities, receivables, and all other financial resources under DCS's control.

4 Policy Statements

4.1 General Responsibilities

All employees and contractors are responsible for the proper use, maintenance, and protection of DCS's physical and financial assets.

Employees must ensure that assets are used only for legitimate business purposes and in compliance with applicable laws, regulations, and company policies.

Any misuse, theft, or damage of assets must be reported immediately to a supervisor or the Ethics and Compliance Function.

4.2 Protection of Physical Assets Asset Maintenance:

Asset Maintenance: Employees must ensure that physical assets are kept in good working condition. Regular maintenance schedules should be followed, and any repairs or servicing should be carried out immediately.

Asset Use: Physical assets should only be used by authorized personnel and exclusively for DCS business purposes. Unless explicitly authorized by management, personal use of company assets is prohibited.

Access Control: Access to physical assets, particularly sensitive or valuable items, must be restricted to authorized personnel. Secure storage facilities and protective measures must be used to prevent unauthorized access.

Asset Inventory: A comprehensive inventory of all physical assets must be maintained. Company assets must be classified according to the Asset Classification Guide and recorded in the Asset Inventory. This inventory must be regularly updated to reflect changes such as acquisition, disposal, or transfer of assets.

Removal of Assets from the Company: Equipment, information, or software—if classified as internal use or confidential—must not be taken outside the company premises without the permission of the unit manager responsible for the asset. Information assets permitted to be taken outside the company must be protected under the responsibility of the approving department manager.

Return of Assets: Employees must return all information assets assigned to them upon resignation or termination to the Human Resources and Support Services Directorate or their supervisor.

Disposal and Destruction of Assets: When deemed necessary, information asset owners must dispose of or destroy assets in accordance with the Disposal and Destruction Policy.

4.2.1. Protection of Assets During Remote Work

It is essential to ensure the security of company assets assigned to employees under remote work arrangements, even outside company offices. Accordingly, employees are required to act in accordance with the following principles:

- Use company assets solely for legitimate business purposes and do not allow unauthorized third parties, including family members, to use them.
- Safeguard the assets by taking reasonable physical security measures to protect them against risks such as theft, loss, or damage (for example, keeping them in a locked area when not in use).
- Ensure that company computers and mobile devices are always protected with strong passwords and that their screens are locked when not in use.
- Immediately report any theft, loss, or damage of assets to the manager and relevant departments (Information Technology, Human Resources).

4.3 Protection of Information Assets

To protect all DCS information assets, all employees must act in accordance with the Information Security and Data Protection Policy and relevant procedures and instructions. It is prohibited to use information assets in a way that unnecessarily consumes capacity, degrades system performance, or compromises information security.

Additionally, the following activities are prohibited:

- Downloading non-work-related images, music, videos; sending chain emails; playing games, etc.
- Installing applications on work-assigned computers and electronic devices (tablets, mobile phones, etc.) without going through relevant approval mechanisms
- Using Java applications, ActiveX, and other mobile codes without proper approvals
- Using cryptographic tools (encryption) on personal computers outside the conditions stated in the Asset Classification Guide
- Uploading applications, code snippets, patches, or scripts from portable media without proper approvals
- Using modems, memory cards, portable disks, etc., without proper approvals.

4.4 Protection of Financial Assets

Financial Transactions: All financial transactions must be conducted with integrity and transparency. Proper documentation and approval processes must be followed, and all transactions must be accurately recorded in DCS's financial systems.

Cash Usage and Bank Accounts: Cash and bank accounts must be managed under strict controls. Employees handling cash or managing accounts must ensure that funds are secure and accessible only by authorized personnel. Regular reconciliations must be conducted to detect discrepancies. Payments from bank accounts must be processed with dual control mechanisms.

Expense Management: All expenditures on behalf of DCS must be reasonable, necessary, and properly documented. Employees must adhere to the company's expense policies, including obtaining pre-approvals for major expenses.

Investment and Asset Management: Financial assets must be managed to maximize value while minimizing risk. Investment decisions must align with DCS's financial policies and be approved by the Board of Directors.

4.5 Security Measures

Physical Security: Offices, data centers, and other facilities (where information assets are located or processed) must be secured using appropriate security measures such as locks, surveillance cameras, and alarms. Access to sensitive areas (e.g., server rooms, archives, or sections restricted to authorized personnel) must be controlled and monitored.

Cybersecurity: Financial data and records must be protected against unauthorized access, breaches, and cyberattacks. Employees must comply with all procedures and instructions in the Information Security and Data Protection Policy. Secure methods must be used when processing financial information.

Antivirus Use: Antivirus software specified by the Information Security Officer must be installed and kept updated on all computers. Users must not uninstall antivirus software or disable updates.

Insurance: Where appropriate, DCS shall acquire and manage insurance policies to protect against losses due to damage, theft, or other risks affecting physical and financial assets.

Cybersecurity: Financial data and records must be protected against unauthorized access, breaches, and cyberattacks. Employees must comply with all procedures and instructions in the Information Security and Data Protection Policy. Secure methods must be used when processing financial information.

Antivirus Use: Antivirus software specified by the Information Security Officer must be installed and kept updated on all computers. Users must not uninstall antivirus software or disable updates.

Insurance: Where appropriate, DCS shall acquire and manage insurance policies to protect against losses due to damage, theft, or other risks affecting physical and financial assets.

5 Responsibilities

5.1 Employees

- Use all DCS assets responsibly and report any concerns or issues regarding asset protection to their supervisor
- Comply with the guiding principles and procedures outlined in this policy and other relevant asset management policies

5.2 Managers

- Ensure employees are aware of their individual responsibilities regarding asset protection
- Regularly monitor the use and condition of assets in their department
- Approve, record, and audit major asset transactions (e.g., equipment transfers, disposals, maintenance)

5.3 Finance Directorate, IT, Ethics and Compliance Function

- Maintain accurate records of financial and physical assets
- Conduct regular audits and assessments to ensure compliance with this policy
- Provide guidance and support to employees on best practices in asset protection

6 Monitoring and Implementation

Regular audits will be conducted to assess the effectiveness of asset protection measures and ensure compliance with this policy.

Any violations identified under this policy will be investigated, and corrective and preventive actions will be taken as deemed necessary.

Evaluations related to the implementation of this policy will be conducted as part of regular compliance reporting.

7 Breach of Policy

Violations of this policy may result in sanctions up to and including termination of employment or contracts with external stakeholders. Legal action may be taken in cases involving theft, fraud, or other criminal activities.

8 Reporting and Whistleblower Protection

DCS provides mechanisms for employees, suppliers, and other stakeholders to report concerns about policy violations confidentially and without fear of retaliation.

Employees must report any misconduct or suspicious behavior, regardless of the seniority of the person involved.

Reports can be submitted to the Ethics and Compliance Function via the email address: etik@dcscustoms.com.tr.

DCS allows anonymous reporting and treats such reports with equal seriousness. All reports are handled in accordance with the **Whistleblower Protection Policy**, ensuring confidentiality and protection from retaliation.

DCS commits to investigating all policy violation reports promptly and fairly. If a violation is confirmed, appropriate corrective actions will be taken and efforts will be made to remedy any damage caused.

9 Review and Revision

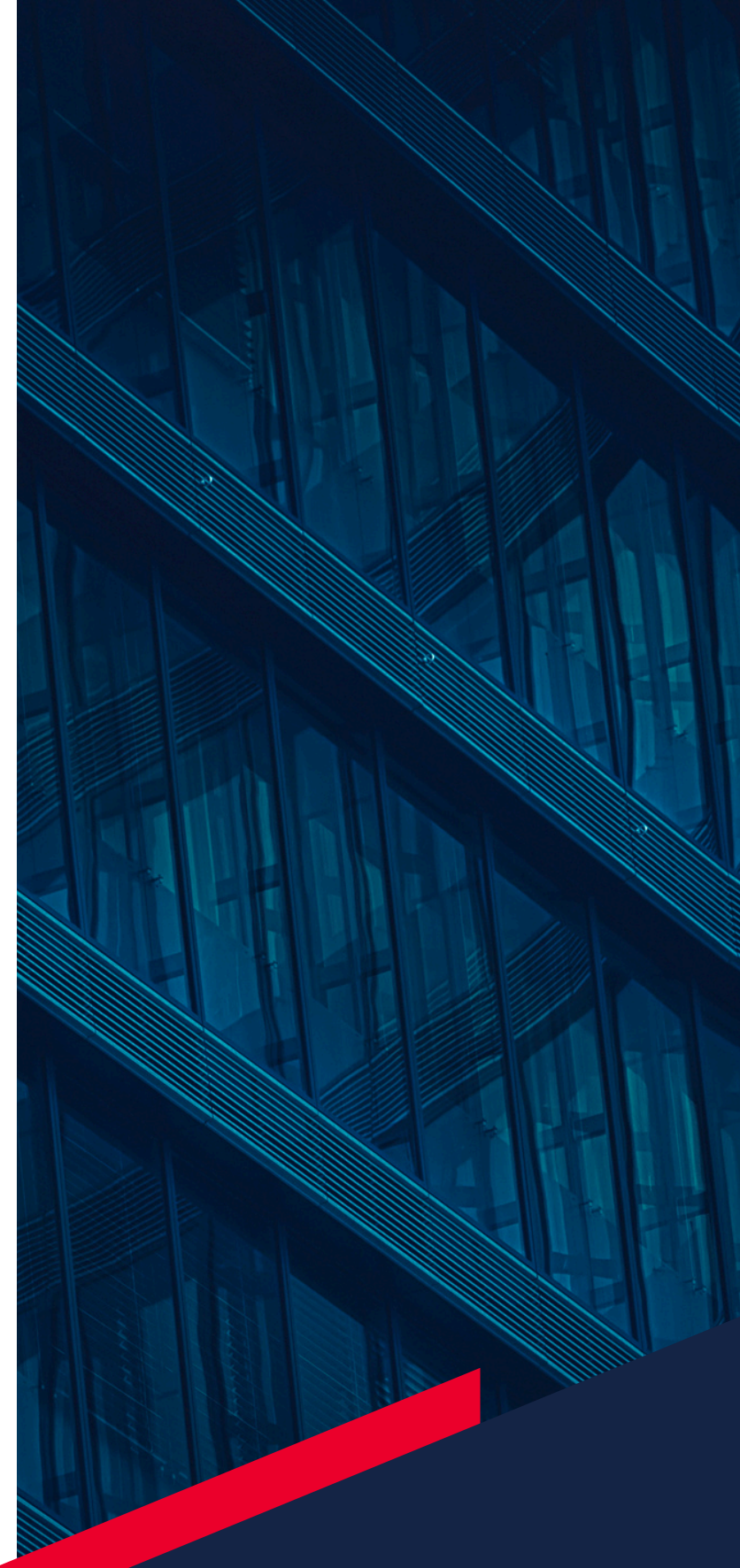
This policy shall be reviewed at least once a year from its effective date to ensure compliance with local and international laws. The review process is carried out in coordination with the Finance Directorate, Information Technology, and the Ethics and Compliance Function. The policy shall be updated as necessary to reflect changes in DCS's operations, asset portfolio, or relevant laws and regulations.

When reviewing the adequacy and effectiveness of the document, security incidents resulting from improper or unauthorized use of assets or from insufficient staff awareness training shall be evaluated.

Other changes and revisions, apart from the annual review, shall be submitted to the Board of Directors for approval through a reasoned change or revision proposal prepared by the Ethics and Compliance Function based on the company's relevant risk assessments. Once approved by the Board, the policy becomes effective and is recorded via the document management system.

DCS

Compliance Program



www.dcscustoms.com.tr