INFORMATION SECURITY AND DATA PROTECTION POLICY

DCS

Compliance Program

Information Security and Data Protection Policy

1 Purpose

The DCS Information Security and Data Protection Policy outlines the measures and responsibilities required to protect the confidentiality, integrity, and availability of information within DCS.

This policy aims to ensure full compliance with applicable data protection legislation and to create a reliable environment for the secure processing of personal, sensitive, and customer data.

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

2 Scope

This policy is based on the control guidelines specified in the ISO/IEC 27001:2022 International Information Security Management standard.

It applies to all employees, contractors, consultants, third-party partners, and any other persons or organizations with access to DCS information systems or data.

It covers all types of data—electronic, physical, and verbal—as well as all systems and processes used to manage, store, or transmit such data.

All business processes and related procedures must be prepared, implemented, and audited in accordance with this policy.

3 Definitions

Information Security: The practice of protecting information by reducing risks to its confidentiality, integrity, and availability.

Information System: Includes all servers, clients, network infrastructure, data, and computing components owned or managed by the company. It also encompasses internal and external services such as internet access and email.

Information Assets: In the context of this policy, this includes information systems, written documents, equipment, phones, portable computers, and stored data.

Data Protection: Legal and regulatory measures to protect personal data against unauthorized access, use, disclosure, or destruction.

Personal Data: Any information relating to an identified or identifiable individual, such as names, contact details, ID numbers, and financial information.

Confidential Information: Proprietary information specific to DCS or its clients, including trade secrets, business strategies, and other sensitive data.

Data Breach: A security incident resulting in unauthorized access to, disclosure, alteration, or destruction of data.

4 Policy Statements

4.1 General Information Security

DCS is committed to protecting its information assets against unauthorized access, use, alteration, disclosure, or destruction. All employees are responsible for complying with information security policies and implementing necessary security measures.

Information assets must be used solely for the conduct of company activities. Access to DCS information systems and data is restricted based on roles and job requirements; only authorized individuals are granted access to relevant information.

Each information asset must have an owner identified in the asset inventory. The asset owner is responsible for maintaining the confidentiality, integrity, and availability of the asset. Users of information systems may only access information assets within the scope of permissions defined by the asset owner, and these permissions must be used strictly for their intended purpose.

Authentication is required before access to sensitive systems or data is granted. Strong authentication methods such as multi-factor authentication (MFA) must be used.

4.2 Prohibited Actions

User Account Restrictions:

Users may not attempt to bypass, disable, or deactivate any information security measures.

Users must not directly or indirectly share their access credentials or allow others to use their access rights. For example, usernames and passwords must never be shared with third parties.

Each user account is exclusive to the designated personnel, who are fully responsible for all access and actions performed using that account.

Software Installation Restrictions:

Users may not install any software on company computers independently. If a user requires software installation, they must submit a formal request via their manager to the IT Department, clearly stating the need and justification.

Requests will be evaluated by the IT Department and senior management. If approved, necessary licenses will be acquired, and software will be installed only by a System Support Specialist.

Users are required to submit a list of all software installed (beyond the operating system) on their assigned devices to the IT Department annually for approval.

4.3 Data Protection Compliance

DCS commits to full compliance with ISO/IEC 27001:2022 Information Security Management System Standard, the General Data Protection Regulation (GDPR) of the European Union, the Turkish Personal Data Protection Law (KVKK), and all relevant local legislation. Accordingly, personal data must be processed lawfully, fairly, and transparently.

Personal data may only be collected and processed for clearly defined and legitimate purposes and must not be used in ways incompatible with those purposes.

DCS will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated with processing personal data. All processes involving personal data must comply with this policy, the "Personal Data Protection and Processing Policy," and the "Personal Data Deletion, Destruction, and Anonymization Policy."

4.4 Data Collection and Use

DCS will collect personal data solely for legitimate business purposes or in compliance with legal obligations. Data subjects will be informed clearly and transparently about the purpose of data collection and how their data will be processed.

Collected personal data must be accurate, complete, and up-to-date. Incorrect or outdated data must be promptly corrected or deleted.

Personal data will be retained only for the duration necessary to fulfill the intended purpose or as required by relevant legislation.

Details on the principles and procedures for processing personal data are further specified in the Personal Data Protection and Processing Policy.

4.5 Data Storage and Security

All data stored electronically or physically must be protected against unauthorized access, loss, corruption, or destruction using appropriate methods. This includes encryption, access controls, and secure physical storage.

Personal data, confidential information, and other sensitive data types must be stored in compliance with security policies to ensure confidentiality, integrity, and availability. Encrypted storage methods are preferred for such data.

To maintain data availability in case of data loss, system failure, or similar incidents, critical data must be backed up regularly. Backup procedures must be tested and configured to allow for rapid recovery.

4.6 Data Access and Confidentiality

Access to personal data and confidential information must be restricted to authorized individuals who require access for their job responsibilities. Role-based access control and necessary technical measures will be implemented.

All employees are required to sign confidentiality agreements as part of their employment, acknowledging their responsibility to protect DCS's information assets.

Employees must not share personal data or confidential information within or outside the company with unauthorized individuals under any circumstances. This obligation remains in effect even after termination of employment.

4.7 Data Sharing and Transfer

When sharing company data, personal data, or confidential information with third parties, data processing agreements, confidentiality clauses, and other suitable safeguards must be in place.

International data transfers must fully comply with applicable data protection legislation. Appropriate technical and administrative measures must be implemented to ensure data security, and data should be transferred only to countries with an adequate level of protection.

Principles and procedures related to the sharing and transfer of personal data are outlined in the Personal Data Protection and Processing Policy.

4.8 Data Disposal

Company data, personal data, or confidential information must be destroyed using appropriate methods once retention periods have expired or processing purposes are no longer valid. Destruction methods such as physical shredding, digital wiping, or data masking must ensure permanent irreversibility.

Where data must be anonymized, identity-related information must be irreversibly separated, and the anonymization process must be carried out in accordance with legal requirements.

Details regarding the disposal and anonymization of personal data are defined in the Personal Data Deletion, Destruction, and Anonymization Policy.

4.9 Password Security Measures

Users are required to comply with the following password guidelines:

- Passwords must not be shared with anyone, including system administrators and company managers.
- Passwords may only be stored in sealed envelopes in secure, locked locations under exceptional circumstances.

- Passwords may be stored and managed using IT-approved Vault software to allow secure access by authorized personnel. The security and management of this software is the responsibility of the IT Department.
- Passwords must be changed regularly, at least once a month.
- Passwords must be changed immediately if they are suspected of being compromised.

Strong passwords must meet the following criteria:

- Minimum of 8 characters
- At least one number (e.g., 123456)
- At least one uppercase and one lowercase letter (e.g., Aa)
- Must not contain dictionary words or their reversals in any language (e.g., cat, tac)
- Must not include personal information (e.g., date of birth, address, relative's name, favorite team)
- At least the last three used passwords must not be reused
- Passwords must be changed upon initial login
- Passwords must not be saved using “remember my password” features
- Personal-use passwords must not be used for work purposes
- Accounts will be locked after 10 consecutive incorrect password attempts

4.10 Internet Security Measures

Internet access must be made solely through the company’s local network infrastructure, protected by firewalls and other security mechanisms. Direct internet access via modems, mobile internet, or wireless networks is prohibited.

DCS reserves the right to block specific websites for individual users, groups, or all users as necessary. Users seeking access to blocked websites must submit a written request to the IT Department, including justification. Users may not bypass these restrictions.

4.11. Insider Trading

DCS adopts a zero-tolerance policy toward insider trading. The scope of insider information extends beyond those defined under Turkish law and includes information that may affect capital market instruments. Sharing or using financial performance data, strategic plans, projects, client and supplier information, mergers, acquisitions, or partnership agreements for personal or third-party benefit constitutes insider trading.

Employees are strictly prohibited from using confidential, financial, or commercial information accessed as part of their duties for personal gain or to benefit third parties. DCS commits to informing all employees, business partners, and relevant stakeholders about insider trading and taking all necessary precautions.

4.12 Incident Response and Data Breaches

DCS will maintain an incident response plan to address data breaches and other security events. This plan will outline steps to contain and mitigate the breach and the process for notifying affected parties and regulators as legally required.

Employees must promptly report suspected data breaches or security incidents to the IT Security Team or the Data Protection Officer (DPO).

DCS will conduct a thorough investigation to determine the cause and impact of any data breach and implement corrective actions to prevent recurrence.

4.13 Employee Training and Awareness

All employees will receive basic training on information security and data protection during onboarding. These trainings will be supported by periodic refresher courses throughout employment.

Training programs will cover secure data processing, recognition and reporting of security breaches or suspicious behavior, and best practices for compliance with data protection laws.

The aim is to increase employee awareness and establish a strong security culture across the organization.

5 Responsibilities

5.1 Employees and Contractors

- Comply with this policy and follow all procedures related to information security and data protection
- Immediately report all security incidents or suspected breaches to the IT Security Team or DPO
- Ensure personal data and confidential information is handled and protected in accordance with this policy

5.2 IT Security Team

- Implement and maintain security measures to protect DCS information systems and data
- Monitor systems for potential security threats and respond promptly to incidents
- Provide guidance and support to employees on best practices in information security

5.3 Data Protection Officer (DPO)

- Oversee DCS's data protection strategy and ensure compliance with applicable data protection laws
- Manage data subject requests and responses to data breaches
- Conduct regular audits to assess compliance with this policy and identify improvement areas

6 Monitoring and Compliance

Regular audits and evaluations will be conducted to ensure compliance with this policy and to identify potential vulnerabilities in DCS's information security practices.

All personnel, suppliers, or third parties who come into contact with information systems and/or data must report weaknesses, security incidents, or conditions that could lead to such incidents in accordance with the incident management procedure. All violations of this policy will be investigated, and appropriate corrective actions—including disciplinary action—will be taken.

7 Breach of Policy

Failure to comply with this policy may result in severe consequences, including termination of employment or business relationships. In cases of gross negligence or deliberate misconduct, legal action may be taken.

8 Reporting and Whistleblower Protection

DCS provides the necessary mechanisms for employees, suppliers, and other stakeholders to report violations of this policy confidentially and without fear of retaliation. Employees must report any misconduct or suspicious activity—even if it involves senior personnel.

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

DCS allows employees to report anonymously and treats all such reports with the same level of seriousness. All reports will be handled confidentially and in accordance with the **Non-Retaliation Policy** to ensure the protection of whistleblowers.

DCS is committed to investigating all reported violations fairly and promptly. If a violation is confirmed, appropriate corrective measures will be implemented to remedy any harm caused.

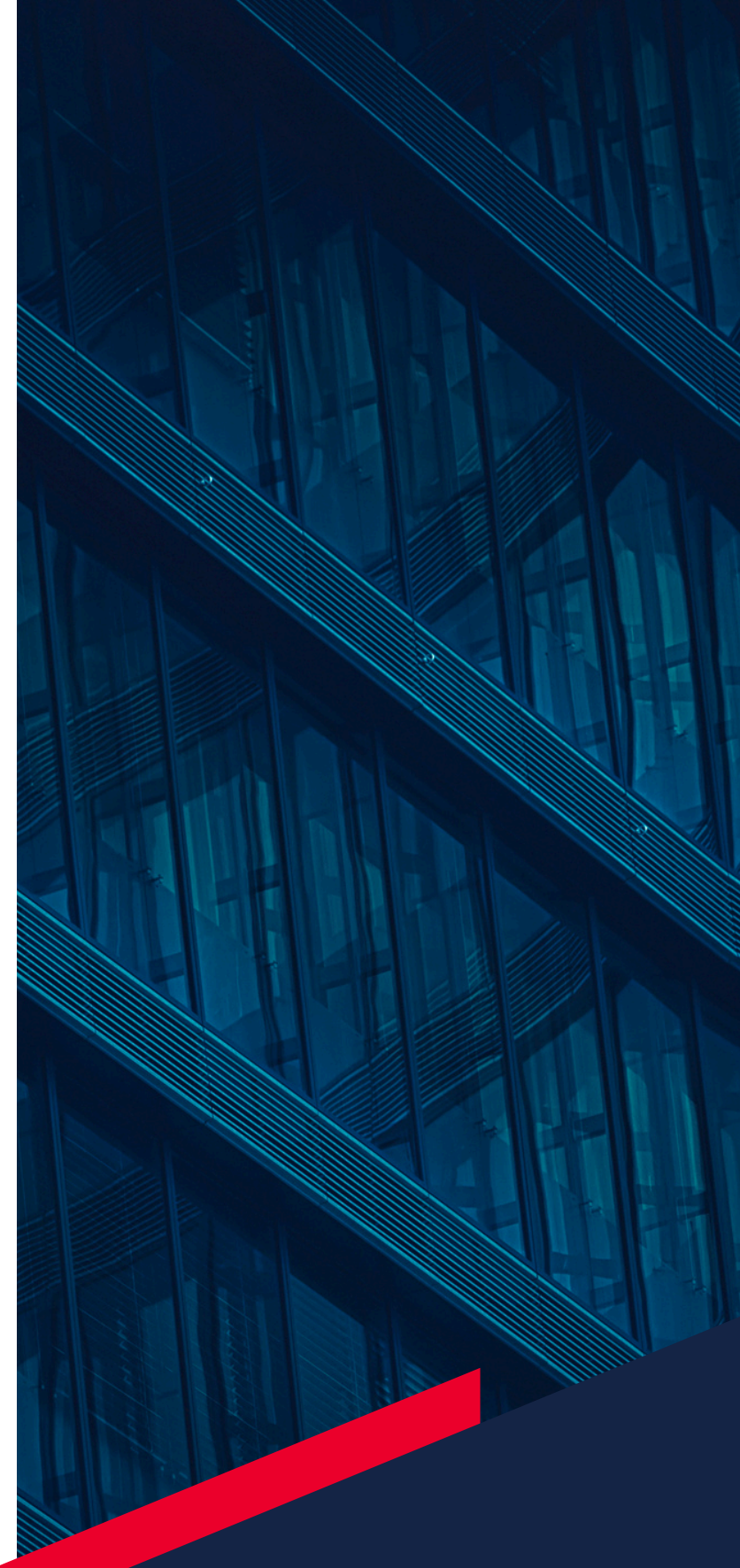
9 Review and Revision

This policy shall be reviewed at least annually from the effective date for compliance with local and international laws. The review process shall be carried out by the IT Department in coordination with the Compliance Function. The policy shall be updated as necessary to reflect changes in technology, legislation, and DCS business practices.

Other changes and revisions shall be submitted to the Board of Directors for approval through a reasoned change or revision proposal prepared by the Compliance Function based on IT evaluations. Once approved by the Board, the policy shall be recorded via the document management system.

DCS

Compliance Program



www.dcscustoms.com.tr