DTC
DIGITAL TRADE CORRIDOR
A MEMBER OF THE PSA GROUP

2024

Global DTC Information Security Policy

Almaty, Kazakhstan

Table of contents

1 | Introduction and general overview

1.1. Policy Objectives

The main objectives of the Information Security Policy are:

- To define the general security policy for DTC Information Systems and the information stored, processed and transmitted by them, including outsourced services.
- To define a uniform approach, ensuring a high degree of information systems security throughout DTC.
- To define responsibilities with regards to Information Systems security.

This document defines the general framework deriving to specific security policies and system specific security standards, as well as departmental/local procedures. All derived security policies, standards, guidelines and procedures shall be consistent with the present policy document.

1.2. Scope of the Policy

This policy applies to all DTC staff, assignees and contractors that provide services to DTC and is an integral part of the DTC Business Code of Conduct.

This policy covers the security of information systems and data networks owned or used by DTC as well as the information that is stored, transmitted or processed by those systems.

This policy does not cover issues related to general physical and building security. It covers, however, physical security aspects of buildings or parts of buildings that directly affect the security of information owned by DTC.

2 | Policy

This document is dedicated to our Stakeholders, inclusive of our Personnel, Customers, Partners and Competent Authorities.

We recognize the critical importance of Information Security, regarding their confidentiality, integrity and availability. Key objectives include:

- To respect, when carrying out professional activities, the safety requirements that derive from the project specifications, contractual agreements and, where applicable depending on the scope of the specific project and the criticality of the object to be developed, the requirements defined by Customer reference.

- To ensure, in the management and execution of any project/service regardless of its type, compliance with the principles underlying information security.

- To define and apply a methodology for analyzing and evaluating the risks connected to the company's core business in order to identify threats and vulnerabilities of its Information Security Management Systems (ISMS) and implement the appropriate countermeasures.

- To ensure that the ISMS involves the entire company organization, workers will be sensitized and trained to carry out their tasks safely and to assume their ISMS responsibilities in this regard.

- To promote the continuous improvement of safety and prevention with monitoring activities in line with the ISMS system.

- To provide, in agreements with third parties, security requirements through contractual clauses aimed at guaranteeing the integrity, availability, confidentiality and non-disclosure of company information, in the interests of the DTC itself and the client companies.

- To control, through a monitoring system, the implementation of the ISMS in the work activities of its resources, verifying compliance with legislative and regulatory provisions regarding information security.

- To periodically review, at least annually, the security policy and the ISMS system, and in the event of significant changes regarding information security.

- To provide for periodic and independent checks, at least annually, regarding the implementation aspects of the ISMS, also activating and participating in specific coordination meetings.

- To raise awareness among company functions of information security issues.

These set the ground rules under which DTC operates and safeguards its data and information systems to both reduce risk and minimize the effect of potential incidents.

2.1. Data Protection

DTC takes the protection of personal data seriously and the security measures set forth in this policy are essential to ensure the data protection standards supporting the DTC Information Management Policy are met.

2.2. Human Resources security

Job definition and resourcing

Information security must be covered in the DTC Security Human Resources policy and standards. The HR policies should ensure, as a minimum, that security is adequately covered in job descriptions; that personnel are adequately trained and that confidentiality agreements are signed by all new employees and contractors.

User training on Security Awareness

A training plan and training material in place to ensure that the right level of Security Awareness is created and maintained within the organization. Software developers and all other relevant personnel involved in the development of software for DTC are required to undertake secure development training on a periodic basis.

2.3. Information Management

Information Classification

The DTC Information Security Policy focuses on the protection of the 3 components of information stored on DTC systems: Confidentiality, Integrity & Availability, whilst ensuring Data Privacy.

All DTC information must be classified based on these 3 categories in order to allow implementation of the appropriate levels of protection in line with its criticality and to ensure that the controls applied to it are sufficient and do not impair the company's business.

Information classification requirements are **detailed in the DTC Information Management Policy.**

Information Handling

Information, in electronic and physical formats, should be handled in accordance with the sensitivity, risk and classification of the information:

- Ensure confidentiality agreements are in place before sharing data externally.
- Check email addresses prior to sending any files.
- Files are NOT to be copied to removable storage.
- Use restricted access storage areas whenever possible.
- Data disposal should be done in accordance with the **Information Asset Handling and Protection Standard for End User.**

2.4. User Authentication Standard

Users must be forced to change their passwords during the first log on, and at 60 - day intervals.

Passwords shall not be displayed or transmitted in clear text and shall be suitably protected via approved cryptographic solutions.

Passwords shall be stored in an encrypted format. A history of passwords shall be maintained to prevent the re-use of passwords.

A maximum of six successive login failures shall result in account lockout until an administrator unlocks it.

Default accounts shall be disabled and/or default passwords associated with such accounts shall be changed.

2.5. Business Application Management Policy

At DTC we have a high dependency on software to conduct our day-to-day business:

- Applications should comply with the Privacy by Design principle.
- A Data Privacy Impact Assessment (DPIA) should be completed for major software changes that involve personally identifiable information (PII).
- Security requirements for software should be documented as part of the development process.
- Software changes should be subject to change control procedures.
- Only authorized users are permitted to deploy software changes.

This policy applies to software we develop for our customers.

2.6. Licensing

DTC uses software from a variety of third parties, copyrighted by the software developer and, unless expressly authorized to do so, employees do not have the right to make copies of the software. The DTC policy is to respect and adhere to all

computer software copyrights and to adhere to the terms of all software licenses to which DTC is a party.

Also, the DTC policy is to manage its software assets and to ensure that DTC installs and uses only legal software on its workstations and servers, in line with the detailed requirements from the IT Asset Management Standard for Software.

2.7. Encryption

Encryption is required to be used to protect all Company data and information from being disclosed to unauthorized parties. All personnel are responsible for assessing the confidentiality level of data being sent or residing on the devices they use. All DTC employees are responsible to comply with the Encryption Standard.

2.8. Backup

DTC Business Continuity Management Policy provides a framework for ensuring that information in scope of this policy will not be lost during an incident affecting availability or integrity. Similarly, all media containing backups of DTC data must be protected according to the data classification related to Data Confidentiality, Integrity & Availability, whilst ensuring data privacy.

Both data classification and backup requirements must be determined by the asset owner and communicated to IT for implementation. Asset / data owners are responsible to inform IT in writing of the specific backup requirements for each asset or data set and of the required backup retention period in line with DTC Business Continuity Management Policy (BCMP).

2.9. Third Party Risk Management Policy (incl. Cloud Computing)

Third Party Risk Management policy defines requirements for carrying out an IT activity with any outsourced external service provider, including Cloud Computing. The process and controls needed to reduce the risks associated with IT outsourcing initiatives, including Cloud Computing arrangements, are detailed in the DTC IT Outsourcing Policy. DTC IT Outsourcing Policy applies equally to all DTC employees and contractors who use any outsourced external IT Service provider.

2.10. Malware Protection

A process must be maintained to ensure that malicious software cannot enter the group’s secure IT environment. This will include regular anti-malware updates,

schedule malware scans and monitoring of events and incidents related to malware, detailed in DTC Threat and Incident Management Policy.

2.11. Security Incident Management Standard

DTC follows a consistent and effective process to address any actual or suspected security incidents relating to information systems and data. Security Incident Management Standard details the framework for early detection, reporting and responding to security incidents.

All security incidents whether actual or suspected, must be reported immediately by sending an email to security@dtcglobal.com.

Even if a Security Incident is not considered to be serious, it should always be reported as it may be part of a wider issue or trend. Additionally, first appearances of the severity of the Security Incident may be deceptive and not indicative of the severity of the underlying risk.

Therefore, ALL Security Incidents must be reported immediately.

2.12. Business continuity management

DTC maintains a Business Continuity Management Policy (BCMP). This requires sub-functions to develop detailed business continuity plans under its umbrella. The IT function must ensure that the Business Continuity Plan adequately addresses business continuity of the DTC IT environment.

2.13. Disaster recovery planning (DRP)

Disaster recovery plan is a subset of BCP. Given the importance of this aspect of the BCP, the key attributes of a disaster recovery plan are discussed below. There are various categories of disruptive events covered by our BCP/DRP:

- Loss of data, which may include loss of program and system files;
- Unavailability of computer and network equipment;
- Environmental disasters;
- Organized/deliberate disruption;
- Loss of utilities/services;
- Equipment/system failure;
- Pandemics;
- Cyber Attacks;
- Other (health and safety, legal, etc.).

Recovery requirements must be determined by the asset owner based on the criticality of the processes of the Business Functions that use the IT systems (determined through Business Impact Analysis). The asset owner will ensure the following:

- Sufficient documentation of each Disaster Recovery Plan, needed to enable efficient execution of the plans.
- Disaster Recovery Plan which specifies the appropriate security measures to ensure the degree of confidentiality and integrity required for the recoverable systems.
- That the Disaster Recovery Plan specifies a regular procedure for making copies of data from which to recreate originals in case of a disaster. Disaster backups should not be used for operational recovery.
- The Disaster Recovery Plan must be tested on a periodic basis.

2.14. Risk Management Policy

Our Information Security Risk Management framework is key to the way in which we identify and treat Information Security risks. Our approach is centrally managed but depends on regional and divisional support; therefore, all employees and external contractors should be familiar with the Risk Management Policy and of their role within the framework.

3 | Responsibilities

3.1. Security Officer

The Security Officer is responsible for:

- Information security management within DTC, acting as a central point of contact on information security for both staff and external organizations.
- Managing and implementing this policy and related policies, standards and guidelines.
- Monitoring and responding to potential and/or actual security breaches.
- Ensuring that staff are aware of their responsibilities and accountability for information security.
- Providing specialist advice on security issues; Ensuring that all staff, permanent, temporary and/or contractors, are aware of the information security policies, procedures and user obligations applicable to their area of work and of their personal responsibilities for information security.

- With Management and HR, determining the level of access to be granted to specific individuals.
- Ensuring staff have appropriate training for the systems they use.
- Ensuring staff know how to access advice on information security matters.

All DTC users are responsible with adhering to the provisions of this Policy and all related policies, standards, guidelines and procedures and must report every incident of misuse or abuse of which they become aware as described in the **DTC Security Incident Management Policy.** Information Security is everyone's responsibility.

3.2. External contractors

All contracts with external contractors that allow access to the organization's data or information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organization comply with all appropriate security policies to protect the data of DTC and its clients.

4 | Breaches

Breach of this Policy will be taken seriously and may result in disciplinary actions in conformity with the legal and contractual framework, including termination of employment. In the case of breaches by external contractors, appropriate action will be taken, which may also include termination of the contract and/or refusal to renew the contract.

Any user disregarding the rules set out in this Policy or in applicable laws will be fully liable and DTC will disassociate itself from the user as far as legally possible.

All breaches of this policy must be reported to the CEO for appropriate action.

All security incidents whether actual or suspected, must be reported as soon as possible.

5 | Revision

Document history:

Author	Version	Date	Signature

Askhat Akhmadiyev *Cybersecurity Officer*	V1	22.04.2024	
Bayan Konirbayev *Chief Technology Officer*	V1	25.04.2024	
Weetan Yeong *Chief Executive Officer*	V1	25.04.2024	