

Pakistan Supply Chain Security (PSCS) Code

1.0 Introduction

Following September 11, 2001 incident, the attention of international community has been focused on security. Supply chain is considered one of the areas which can pose a security threat and could be utilized by the terrorists. In this context United States of America Homeland Security Department has introduced Container Security Initiative (CSI) and Customs-Trade Partnership against Terrorism (C-TPAT) to ensure its supply chain security. The International Maritime Organization (IMO) has introduced International Ship and Port Facility Security (ISPS) Code. To ensure security of supply chain of Pakistani exporters a voluntary scheme named Pakistan Supply Chain Security (PSCS) Code is introduced.

By adopting Pakistan Logistic Supply Chain Security (PSCS) Code Pakistani enterprises re-iterate their commitment to meet expectations of their clients and provide a secure supply chain link for their local and foreign trade partners.

PSCS Code is developed by the members of Logistic Security Working Group of National Trade and Transport Facilitation Committee (NTTFC) and approved in the meeting of NTTFC held on 2nd April, 2005 under chairmanship of the Secretary, Ministry of Commerce.

2.0 Scope

PSCS Code may be adopted by the enterprises on voluntary basis. It outlines best practices for managing supply chain security in Pakistan. It is useful for manufactures, exporters, road transporters, warehouse operators and freight forwarders.

3.0 Objectives

The objective of PSCS Code is to provide a framework to the enterprises involved in manufacturing, storage and logistic supply chain for operating in a secure manner; providing location security, theft prevention, shipping and receiving controls, information security and internal controls for detecting and correcting security problems.

4.0 Definitions and Terms

1. Company security plan means a plan developed to ensure the applications of all measures designed to protect the facility, persons, machinery, merchandise and vehicle from the risks of security incidents.
2. Company security officer means the person designated by the company for ensuring that a facility security assessment is carried out; that a company security plan is developed, submitted for approval, and thereafter implemented and maintained. He will keep liaison with relevant security personnel and agencies and keep himself abreast of security situation of the company.

3. The term "facility" means factory, office, haulier base, warehouse or any place where processing of a product or service is being carried out by the company.

5.0 General Requirement

The organization shall establish, document, implement and maintain a security management system and continually improve its effectiveness in accordance with the requirement of this code.

5.1 Management Responsibility

5.1.1 Management Commitment

Top management shall provide evidence of its commitment to the development and implementation of the security management system and continually improving its effectiveness by:

- a) communicating to the organization the importance of security as well as meeting statutory and regulatory requirements;
- b) establishing the security policy;
- c) conducting security reviews; and
- d) ensuring the availability of resources.

5.1.2 Security Policy

Top management will ensure that the security policy:

- a) is appropriate for the needs of the organization with adequate emphases on protecting people, property and operational practices against loss by intentional destruction or theft;
- b) includes a commitment to comply with requirements and continually improve the effectiveness of the security management system; and
- c) is reviewed for continuing suitability.

5.1.3 Security Officer

Top management shall appoint a security officer who, irrespective of other responsibilities, shall have the responsibility and authority that includes those mentioned in 4.0.2 and the following:

- a) ensuring that processes needed for the security management are established, implemented and maintained;
- b) reporting to top management on the performance of security management system and any need for improvement; and
- c) ensuring promotion of awareness of supply chain security throughout the organization.

5.1.4 Internal Communications

Top management shall ensure that appropriate communication processes are established within the organization and that communication takes place regarding the promotion and effectiveness of the security management system. Suggestions for improvement from the employees shall be encouraged.

5.1.5 External Communications

Top management shall establish appropriate process to ensure that the organization's security requirements are appropriately communicated to its suppliers and shippers and followed by them.

5.1.6 Provision of Resources

The organization shall determine and provide the resources needed to implement and maintain security management system and continually improve its effectiveness.

5.1.7 Security Reviews

Top management shall review the organization's security management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. The review shall include assessing the opportunities for improvement and the need for changes to the security management system, including the company security plan.

5.1.8 Executive Leadership

Top management shall play the leadership role in organizing the security management system and actively participate in local supply chain related security meetings, conferences and seminars.

5.2 Location Security and Theft Prevention

5.2.1 Location Security Assessment

Location security assessment is an essential and integral part of the process of developing and updating the company security plan. The security officer shall ensure that the location security assessment is carried out by the persons with appropriate skills to evaluate the security of the facility of the company. The location security assessment shall include an on-scene security survey and at least the following elements:

- a) identification of existing security measures, procedures and operations;
- b) identification of the key operations that need to be protected;
- c) identification of possible threats to the key operations and the likelihood of their occurrence, in order to establish and prioritize security measure; and
- d) identification of weaknesses, including human factors in the infrastructure, policies and procedures.

The location security assessment shall be documented, reviewed, accepted and retained by the company.

5.2.2 Access Control

- a) Unauthorized access to the facility and conveyance shall be prohibited. The organization shall take measures to monitor entry and movement of people and vehicles to the facility as a security precaution. Positive identification of all employees, visitors and vendors shall be ensured.
- b) The allotment and duplication of keys to building(s), vehicles and storage areas shall be controlled.

5.2.3 Physical Security

All building and yards shall be constructed of materials which resist unlawful entry and protect against outside intrusion. Physical security shall include perimeter fences, locking devices in external and internal doors, windows, gates and fences, adequate lighting inside and outside the facility, and segregation and marking of international, domestic, high value, and dangerous goods within the warehouse by a safe, caged or otherwise, fenced-in area.

5.2.4 Security Inspections and Audit

The organization shall undertake a security audit of the facility and operations to verify their compliance with the security plan at least annually.

Regular inspections shall be conducted to protect against introduction of unauthorized personnel and material.

5.2.5 Security Plan

- a) The organization shall prepare a security plan approved by the top management.
- b) In absence of the required competency to prepare the plan the organization shall engage a competent security agency to carry out this task. In such cases the competent security agency shall undertake the review and approval of company security plan or its amendments, for a specific location/facility.
- c) The submission of a company security plan, or amendments to previously approved plan, for approval shall be accompanied by the location security assessment on the basis of which the plan, or the amendment, is submitted for review.
- d) The plan shall be written in Urdu or English and should address the following:
 - i. Measures designed to prevent intrusion of weapons, dangerous substances and devices intended for use against people, facility, merchandise and the carriage of which is not authorized in the facility;
 - ii. Identification of the restricted areas and measures for the prevention of unauthorized access to them;
 - iii. Measure to prevent unauthorized access to the facility;
 - iv. Procedures for responding to any security threat or breaches of security, including provisions for maintaining critical operations of the facility;

- v. Procedure for evacuation in case of threat or breaches of security;
 - vi. Duties of the security related personnel and other facility staff related to security;
 - vii. Procedures related to the audit/inspection of the security activities;
 - viii. Procedure for periodic review of the plan for updating;
 - ix. Procedure for reporting security incident;
 - x. Identification of company security officer including 24 hour contact details;
 - xi. Procedure to ensure the inspection, testing, calibration and maintenance of security equipment provided in the facility (if applicable);
 - xii. Identification of the location where the security equipment is provided; and
 - xiii. Procedures, instructions and guidance on the use of the security alert system, including the testing, activation, deactivation, resetting and limiting false alerts.
- e) Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the company.
 - f) The management shall determine which changes to the approved security plan or to any security equipment specified in an approved plan shall not be implemented unless the relevant amendments to the plan are approved by the management.
 - g) The nature of the changes to the company security plan or the security equipment that have been specifically approved by the management shall be documented in a manner that clearly indicates such approvals.
 - h) The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction and amendments.

5.2.6 Information Security

The organization shall ensure protection of computer information from unauthorized use.

5.2.7 Personnel Security

The organization shall conduct employment screening and interviewing of prospective employees to include periodic background checks and application verification.

5.3 Shipping and Receiving Controls

The organization shall establish and maintain an appropriate procedure to ensure that its vendors/suppliers have suitable arrangements in place to eliminate delivery of unauthorized items.

The organization (if applicable) shall take measures for handling of incoming and outgoing goods. This shall include protection against introduction, exchange or loss of any legal or illegal material. Security controls shall include:

- a) Having a designated security officer to supervise receipt and dispatch of cargo;
- b) Properly marked, weighed, counted and documented products;
- c) Procedures for verifying seals on containers, trailers and railcars;
- d) Procedure for detecting and reporting shortages and overages;
- e) Procedure for tracking and timely movement of incoming and outgoing goods;
- f) Proper storage of empty and full containers to prevent unauthorized access; and
- g) Procedure for notifying to law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.

It shall be ensured that all the transport documents are complete, legible and accurate and submitted to relevant authority on timely basis.

5.4 Reporting System

- a) The organization shall establish a documented system for reporting, recording and investigating non-conformances regarding:
 - i. Security incidents;
 - ii. Potential security hazards;
 - iii. Un-secure conditions; and
 - iv. Regulatory compliance.
- b) Immediate actions shall be taken to avoid problems pending further investigation. The procedure shall clearly identify the authorized person and his/her replacement in case of the absence of such figure. Each report shall include:
 - i. An investigation to establish the immediate cause of the non-conformance;
 - ii. The identification of the root cause; and
 - iii. Recommendations for corrective actions to prevent recurrence.

5.5 Drills and Exercises

To ensure effective implementation of the company security plan, drills shall be carried out at the appropriate interval taking into account the company type, personnel changes and the location. The company security officer shall ensure effective coordination and implementation of security plan by participating in the exercises at appropriate intervals.

5.6 Training, Awareness and Education of Employees

The organization shall arrange security awareness training to cover all employees in the following topics:

- a) The nature of security risks;
- b) Recognition of security risks;
- c) Methods to address and reduce security risks;
- d) Actions to be taken in case of breach of security;
- e) Recognition of internal conspiracies;
- f) Determining and addressing unauthorized access; and
- g) Maintaining cargo integrity;

The employee shall be provided with refresher courses at appropriate interval and records of the training shall be maintained.

5.7 Records Management

Records shall be established and maintained to provide evidence of conformity to requirements and of the effective operation of security management system. Records shall remain legible, readily available and retrievable. A documented procedure shall be established to define the controls needed for identification, storage, protection, retrieval, retention time and disposition of records.