

SECURE TRADE PARTNERSHIP **SINGAPORE CUSTOMS**

GUIDELINES



Contents

Section		Page
1	Introduction	1
2	Security Management System	2
3	Risk Assessment	3
4	Security Measures	5
5	Appendix A	6

1

Introduction

- 1.1 The Secure Trade Partnership (STP) Guidelines spells out the requirements which companies in the supply chain should adopt to enhance the security of their operations and supply chains. Companies meeting such requirements will be certified as STP companies by Singapore Customs.
- 1.2 Under the STP Guidelines, companies are required to:
 - (a) have security management systems;
 - (b) conduct risk assessments of their business operations; and
 - (c) implement the security measures under the STP Guidelines to secure their supply chains.
- 1.3 The STP Guidelines provides companies with a framework to guide the development, implementation, monitoring and review of their supply chain security measures and practices.
- 1.4 Companies that decide to apply for certification under the STP will self-assess against the STP Guidelines to ensure that their internal policies, processes and procedures are robust.

2 Security Management System

- 2.1 Supply chain security can never be an isolated responsibility of a person or a unit operating within a company. To achieve a robust supply chain security implementation, security must be driven through a holistic company wide effort.
- 2.2 A company is required to establish a security management system to develop, document, implement, maintain and review the company's supply chain security measures and practices. The security management system should include but not be limited to:
- (a) A framework for establishing and reviewing the company's security policy and objectives and commitment to security;
 - (b) A framework for effective communication within the company; and
 - (c) A review process to ensure continuing relevance and improvement.

3 Risk Assessment

- 3.1 The STP encourages companies to develop security profiles and implement security measures based upon a risk assessment of the companies' business models.
- 3.2 A company is required to conduct a risk assessment of its operational processes and supply chain. The company must seek to mitigate the risks and vulnerabilities of its operations within the supply chain.

Manufacturers/Suppliers

- 3.3 Manufacturers and suppliers are usually at the start of the supply chain for finished goods. Raw materials and products leaving their factories/plants have to be properly documented from the very onset so as to minimise exploitable data errors or the need for content verification at later stages of the chain. With accurate manifests, tamper-proof packaging, and well documented handing-over processes, manufacturers and suppliers will be able to hand over their goods to the cargo handling agents such as warehouse operators and transport companies in good shape for them to be moved through the supply chain securely.

Warehouse Operators and Owners

- 3.4 Warehouse operators and owners receive goods from manufacturers, transporters or other intermediaries, store them, and then provide them to other intermediaries, often in a different configuration. They should have a good information system to keep track of all the goods being handled and stored, and be able to provide the relevant information on the goods to the next intermediary in the chain. In addition, their premises should be appropriately secured to ensure that the goods trusted in their care are safe from tampering.

Transporters

- 3.5 Transport operators have a key responsibility in ferrying goods from one point to another. Transport operators should have measures to prevent their transport vehicles from being hijacked or substituted. They should also have a good information system to monitor and track the goods entrusted to them. In addition, transport operators should ensure that their vehicles and the goods being carried by their vehicles are not easily tampered with.

Terminal Operators

- 3.6 Terminal operators have a key responsibility for handling goods and containers prior to loading onto an aircraft or a vessel, and after unloading from an aircraft or a vessel. Essentially they are the last point before departure and first point on arrival for the goods and containers. Their premises should be appropriately secured to ensure that the goods and containers trusted in their care are safe from tampering.

Sea and Air Freight Operators

- 3.7 Sea and air freight operators have a key responsibility in ferrying goods from one point to another on vessels and aircrafts respectively. Sea and air freight operators should have measures to prevent their carriers from being hijacked or substituted while on their journeys. They should have a good information system to monitor and track the goods being entrusted to them. In addition, sea and air freight operators should ensure that their vessels and aircrafts and goods being carried on board their vessels and aircrafts are not easily tampered with.

4 Security Measures

- 4.1 The security measures under the STP Guidelines comprise 8 elements that a company must address:
- (a) Premise security and access controls;
 - (b) Personnel security;
 - (c) Business partner security;
 - (d) Cargo security;
 - (e) Conveyance security;
 - (f) Information and Information Technology (IT) security;
 - (g) Incident management and investigations; and
 - (h) Crisis management and incident recovery.
- 4.2 The security measures adopted or implemented must seek to mitigate the risks and vulnerabilities identified from the company's risk assessment process.
- 4.3 Please refer to Appendix A for the Security Measures under the STP Guidelines.

STP Guidelines – Security Measures

1. Premise Security and Access Controls

Access controls and physical deterrents must be in place to prevent unauthorised access to the exterior and interior of companies' facilities. The system must include the positive identification of all employees and visitors at all points of entry.

1.1. Perimeter Fencing

Perimeter fencing and appropriate peripheral barriers should be in place to secure companies' premises. Perimeter fencing should enclose the yard or terminal, especially areas where container, cargo consignment, trailers and other rolling stock are parked or stored. All fencing should be regularly inspected for integrity and damage.

1.2. Gates and Gate Houses

Gates through which all vehicles and/or personnel enter or exit should be manned, monitored or otherwise controlled.

1.3. Parking

Parking access to facilities should be controlled and monitored. Private passenger vehicles should be prohibited from parking in close proximity to cargo handling and cargo storage areas.

1.4. Building Structure

Buildings should be constructed of materials that resist unlawful entry. The integrity of the structures should be maintained by periodic inspection and repair.

1.5. Locking Devices and Key Controls

All external and internal windows, doors, fences and gates should be secured with locking devices or alternative access monitoring or control measures. Management or security personnel should control the issuance of all locks and keys.

1.6. Lighting

Adequate lighting should be provided inside and outside companies' facilities including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.

1.7. Alarm Systems and Video Surveillance Cameras

Alarm systems and video surveillance cameras should be utilised to deter potential intruders from attempting to gain entry, detect possible intrusion, expand the area of security surveillance, and assist in post-incident investigations.

1.8. Restricted Areas

Restricted areas should be clearly identified and monitored to prevent unauthorised access.

1.9. Security Personnel and Organisation

A personnel or unit should be in charge of the security of the company. Companies may engage the services of a security organisation to further enhance the security of their facilities.

1.10. Access Controls for Employees

An employee identification system should be in place for positive identification and access control purposes. For example, employees should be issued with colour photograph identification cards. Employees should only be given access to those areas needed for the performance of their duties.

1.11. Access Controls for Visitors

A visitor-identification and monitoring system should be in place. For example, visitors should present positive identification and register at the security station prior to entry into company premises and visitors should visibly display their temporary identification passes. All visitors should be escorted and only have access to those areas where they have legitimate business.

1.12. Challenging and Removing Unauthorised Persons

Procedures and training should be in place for all employees to report and challenge any unauthorised or unidentified persons.

2. Personnel Security

Procedures must be in place to screen prospective employees and to periodically check current employees. Procedures must be in place for educating and training of employees regarding security policies, recognition of deviations from those policies and understanding of what actions must be taken in response to security lapses.

2.1. Pre-Employment Verification, Background Checks and Investigations

Application information such as employment history, references, and educational records should be verified prior to employment.

Background checks and investigations should be conducted on prospective employees as appropriate and to the extent allowed under national law. Depending on the sensitivity of the job scope and/or job appointment that may compromise companies' operations, a more extensive background checks and investigations should be conducted on prospective employees.

2.2. Periodic Background Checks / Reinvestigations for Current Employees

Periodic checks and reinvestigations should be performed on current employees based on cause, and/or the sensitivity of employees' positions.

Companies should update information in individual personnel files, taking note of any unusual changes in their social and economic situations.

2.3. Education, Training and Awareness

Programmes should be in place to educate and train employees on security requirements including areas such as:

- (a) The company's security policies;
- (b) Recognising potential internal threats to security;
- (c) Maintaining cargo integrity;
- (d) Protecting access controls; and
- (e) Identifying and reporting suspicious cargo, persons and activities.

Such programmes should be included into new employees' induction programme. A refresher course should be built into the programme to keep employees updated on current threats.

2.4. Termination Procedures

Procedures should be in place to expeditiously remove identification, premises and information systems access for employees whose employment has been terminated.

3. Business Partner Security

Companies must work with business partners and obtain their commitment to voluntarily increase their security measures, so as to bolster the security of the global supply chain.

The term "business partners" refers to current and prospective suppliers, manufacturers, service providers, contractors and vendors where companies outsource or contract elements of their supply chains.

3.1. Screening of Business Partners

Procedures should be in place for the screening, selecting, establishing and renewing of relationships with business partners. The procedures should include the conduct of interviews, reference checks and use of information provided by business partners and external resources. For example, business information services, banks and referrals from other organisations.

Screening and selection criteria such as legality, financial solvency and stability, ability to fulfil contractual security requirements, capability to identify and rectify security weaknesses where required may also be used.

3.2. Security Provisions in Agreements / Contracts or Security Declaration

Companies should include security provisions in written agreements and/or contracts with business partners or require business partners to provide a security declaration. The security provision or declaration should describe how goods are safeguarded, how associated information is protected, and how security measures are demonstrated and in place.

Agreements / contracts or security declarations should be reviewed when necessary and/or at least on a regular basis to suit companies' operations and changes in business environment.

3.3. Security Certification

Companies should obtain documentary proof of business partners' participation and certification by a foreign Customs Administration and/or other security programmes.

3.4. Review Business Partners' Adherence to Security Measures

Where appropriate, reviews should be conducted on business partners' processes and facilities to ascertain the validity of business partners' declarations on security. Where the findings are unsatisfactory, companies should communicate the issues to business partners and allow time for the issues to be rectified. Where necessary, companies may wish to reconsider their relationships with such business partners.

4. Cargo Security

Procedures must be in place to ensure that the integrity of cargo is maintained to protect against the introduction of unauthorised materials and/or persons.

4.1. Documentation Processing and Verification

Procedures should be in place to ensure that information in all documentation used in the movement and clearance of cargo, both electronic and manual, is legible, complete, accurate and protected against the exchange, loss or introduction of erroneous information. Companies should check for signs of tampering, forgery or other anomalies.

4.2. Receipt and Release of Cargo

Procedures should be in place to ensure that arriving and departing cargo is reconciled against relevant documents, for example, cargo manifest, packing list, bill of lading, purchase and delivery order. Procedures should be in place to check that cargo is accurately described, weighed, labelled, marked, counted and verified when receiving and releasing cargo. Persons / drivers delivering or receiving cargo should be positively identified before cargo is received or released.

4.3. Signature and Stamp Policies

Procedures should be in place on signature and stamp requirements for critical process handover points, for example, document preparation processes, issue of seals, breaking of seals, physical count of cargo, conveyance inspection, cargo delivery, cargo receipt and counting of unshipped pieces. Documents pertaining to custody and responsibility over cargo transferred or when a service is provided should be signed by the person delivering and receiving it.

4.4. Container Inspection

Procedures should be in place to verify the physical integrity of the container structure, including the reliability of the locking mechanisms of the doors. A seven-point inspection process is recommended for all containers:

- (a) Front wall;
- (b) Left side;
- (c) Right side;
- (d) Floor;
- (e) Ceiling;
- (f) Inside/outside doors; and
- (g) Outside/undercarriage.

4.5. Seals and Markings

Procedures should be in place on how seals and markings are to be controlled, affixed and checked. The following measures are recommended:

- (a) Only designated authorised person(s) should number and distribute seals and markings;
- (b) A log should be kept to record the personnel receiving seals and markings and where they were used; and
- (c) Seals and markings should not be issued in strict numbering sequence to avoid prediction of number.

Container seals should meet or exceed the current PAS ISO 17712 standards for high security seals.

4.6. Storage of Containers and Cargo

Containers and cargo should be stored in a secure area to prevent unauthorised access and/or tampering.

4.7. Inventory Control

Procedures should be in place to control the inventory and storage of cargo. The following measures are recommended:

- (a) Stock-taking;
- (b) Using trained watch service or warehouse staff to visually inspect inventory;
- (c) Requiring step-by-step details of the checks and counter-checks performed by staff; and
- (d) Requiring more frequent inspections during peak receiving period and discrepancy reporting.

5. Conveyance Security

Procedures must be in place to ensure that conveyances are capable of being effectively secured.

5.1. Conveyance Inspection

Procedures should be in place to ensure that potential places of concealment of illegal goods on conveyances are regularly inspected. All internal and external compartments and panels should be secured.

5.2. Tracking and Monitoring of Conveyance

Procedures should be in place to track and monitor accurately activities relating to the movement and handling of cargo both within companies' premises, and at handover points between companies and external parties. The tracking and monitoring system could be via:

- (a) Electronic means. For example, transponders, smart cards, electronic seals, videos, digital photos, mobile phones, radios and Global Positioning Systems (GPS); or
- (b) Activity logs etc.

5.3. Operators' Guide

Operators of conveyances should be trained to maintain the security of the conveyances and the cargo at all times and to report any actual or suspicious incident to designated security department staff. Guidelines should be in place to train operators on:

- (a) Detail route planning for pick up and delivery;
- (b) Confidentiality of load, route and destination;
- (c) Policy on keys, parking area, refuelling and unscheduled stops;
- (d) Reporting for accident or emergency;
- (e) Reporting of any irregularity in loading, locking and sealing; and
- (f) Installation and testing of security alarms and tracking devices, if any.

5.4. Storage of Conveyance

Conveyances should be stored in a secure area to prevent unauthorised access and/or tampering.

6. Information and Information Technology (IT) Security

Procedures must be in place to maintain confidentiality and integrity of data (physical and electronic) and information systems used in the supply chain including protection against misuse and unauthorised alteration.

6.1. Information Security Policy

An information security policy and procedures and/or security-related controls such as firewalls, passwords, anti-virus software and encryption software, etc, should be in place to protect information systems from unauthorised access.

6.2. Information/Document Classification, Handling and Access Controls

Procedures should be in place for classifying information/documents according to their sensitivity and criticality. Important and sensitive information and documents should be stored in a secure area or system which is accessible only to authorised personnel. Regular reviews should be conducted to ensure that rights and privileges granted are appropriate and have not been abused.

6.3. Data Life Cycle Control

Procedures should be in place to control the life cycle of data.

6.4. Data Back-ups and Recovery Plans

Procedures and back-up capabilities should be in place to protect against the loss of information.

7. Incident Management and Investigations

Procedures must be in place to provide a coordinated, structured and comprehensive response to an incident or risk situation and identify root causes so that actions can be taken to prevent recurrences.

7.1. Reporting Incidents

Procedures should be in place for reporting incidents such as shortages and over landing of cargo, irregularity or illegal activities and security breaches to management.

Companies should maintain a database of incident reports, actively monitor and identify trends and patterns for potential security risks and breaches.

7.2. Investigate and Analyse

Procedures should be in place to ensure that incidents are investigated and analysed with the objectives of determining the cause of the incident and implementing the necessary revisions and improvements to prevent the recurrence of such an incident.

8. Crisis Management and Incident Recovery

In order to minimise the impact of a disaster or security incident, crisis management and recovery procedures should be in place. The procedures should include advance planning and establishment of processes to operate under such extraordinary circumstances.

8.1. Contingency or Emergency Plans

Contingency or emergency plans for disaster or emergency security situations should be in place.

The contingency or emergency plans should be communicated to all appropriate employees and regularly updated as operational and organisational changes occur. Companies should conduct periodic training of employees and testing of contingency or emergency plans.

8.2. Business Continuity Plan (BCP)

Companies are encouraged to develop a Business Continuity Plan (BCP) to ensure that Critical Business Functions (CBF) can continue during and after a crisis or disaster affecting their companies or segments of their supply chains.

CONTACT US

For more information on the STP,
please visit our website at www.customs.gov.sg or
email us at customs_scs@customs.gov.sg

Supply Chain Security Branch

Singapore Customs

55 Newton Road #08-01

Revenue House

Singapore 307987



Singapore Customs