

SECURE TRADE PARTNERSHIP **SINGAPORE CUSTOMS**

GUIDELINES AND CRITERIA



Contents

Section		Page
1	Introduction	1
2	Security Management System	2
3	Risk Assessment	3
4	Security Measures	5
5	Appendix A: STP Guidelines	A1-A6
6	Appendix B: STP Criteria	B1-B6

1

Introduction

- 1.1 The Secure Trade Partnership (STP) Guidelines and Criteria spells out the requirements which companies in the supply chain should adopt to enhance the security of their operations and supply chains. To qualify for STP status, companies must meet the requirements under the STP Guidelines. To qualify for the STP-Plus status, companies must meet the requirements under the STP Criteria.
- 1.2 The STP Guidelines and Criteria provide companies with a framework to guide the development, implementation, monitoring and review of their supply chain security measures and practices.
- 1.3 Under the STP Guidelines and Criteria, 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.
- 1.4 Companies that decide to apply for the STP programme will first do a self-assessment against the STP Guidelines or Criteria to gauge how robust their security measures are.
- 1.5 The key differences between the STP Guidelines and the STP Criteria are the minimum criteria which are highlighted in Appendix B: “STP Criteria – Security Measures for STP-Plus Status”.
- 1.6 A company must meet all minimum criteria stated in the STP Criteria before the STP-Plus status could be accorded to the company. For a company who is unable to meet the minimum criteria but is able to fulfil the requirements under the STP Guidelines in Appendix A, the company will be accorded with the STP status.

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 should 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 should conduct a risk assessment of its operational processes and supply chain. The company should 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 and the STP Criteria comprise of 8 elements that a company must address:
- (a) Premises 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 Appendix A contains the Security Measures under the STP Guidelines for STP Status and Appendix B contains for the Security Measures under the STP Criteria for STP-Plus Status..

STP Guidelines – Security Measures for STP Status

1. Premises 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, visitors and vendors at all points of entry.

1.1. Perimeter Fencing

Perimeter fencing should be in place to enclose the areas around cargo handling and storage facilities.

Interior fencing within a cargo handling structure should be in place to segregate high value and hazardous cargo.

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 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. 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.

1.9. Access Controls for Employees

An employee identification system should be in place for positive identification and access control purposes.

Employees should only be given access to those areas needed for the performance of their duties.

1.10. Access Controls for Visitors and Vendors / Contractors

A positive identification system should be in place to manage access control for visitors and vendors/ contractors.

All visitors should be escorted and visibly display identification passes.

1.11. Challenging and Removing Unauthorised Persons

Procedures 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 employees. Procedures must be in place to create awareness for employees, on security and actions to be taken in response to security threats.

2.1. Pre-Employment Verification and Background Checks

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

Background checks and investigation should be conducted on prospective employees as appropriate and to the extent allowed under national law.

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.

2.3. Security Awareness

A security awareness programme should be provided to relevant employees to recognise and foster awareness of security threats.

The security awareness programme should include the following:

- Recognising potential risks
- Maintaining cargo integrity
- Protecting access controls

Employees should be made aware of the procedures the company has in place to address a situation and how to report it.

2.4. Resignation and Termination of Personnel

Procedures should be in place to remove identification cards, as well as premises and information systems access for terminated and resigned employees.

3. Business Partner Security

Companies must work with business partners and obtain their commitment to voluntarily improve 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 and selection of business partners.

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

3.2. Security Requirements for Business Partners

Business partners should demonstrate that they are meeting the company’s supply chain security obligations in any of the following ways:

- through written or electronic confirmation;
- through contractual obligations;
- through a letter from a senior business partner officer attesting to compliance;
- through a written statement demonstrating their compliance with STP or other supply chain security programmes; or
- by providing a completed supply chain security profile.

3.3. Business Partners’ Participation/Certification in STP or Other Related Supply Chain Security Programmes

Company should have documentation indicating their business partners’ status of participation in the Secure Trade Partnership programme, supply chain security programme(s) administered by foreign Customs administrations or in other related supply chain security programme(s).

3.4. Review of Business Partners’ Compliance to Security Requirements

Procedures should be in place to monitor and review business partners’ compliance to security requirements.

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 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.

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 order 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

Procedures should be in place on how seals are to be controlled, affixed and checked.

Only designated authorised person(s) should distribute seals.

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.

5. Conveyance Security

Procedures must be in place to protect the conveyance (e.g. trucks, prime movers, trailers) against the introduction of unauthorised personnel and material.

5.1. Conveyance Inspection

Procedures should be in place to ensure that potential places of concealment on conveyances are regularly inspected.

5.2. Tracking and Monitoring of Conveyance

Procedures should be in place to track and monitor the movement of conveyance carrying the cargo between companies and external parties.

5.3. Drivers' Guide

Guidelines should be in place to train drivers on:

- (a) Inspection of conveyance;
- (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) 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 and information systems used in the supply chain including protection against misuse and unauthorised alteration.

6.1. Information Security Procedures

Information security procedures and/or security related controls should be in place to protect information systems from unauthorised access.

6.2. Accountability

A system should be in place to identify the abuse of IT including improper access, tampering or the altering of business data.

6.3. 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 to management. Incidents include short landing and over landing of cargo, irregularity or illegal activities and security 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 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.

STP Criteria – Security Measures for STP-Plus Status

1. Premises 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, visitors and vendors at all points of entry.

1.1 Perimeter Fencing

Perimeter fencing should be in place to enclose the areas around cargo handling and storage facilities.

Interior fencing within a cargo handling structure should be in place to segregate high value and hazardous cargo.

All fencing must be regularly inspected for integrity and damage.

1.2 Gates and Gate Houses

Gates through which all vehicles and/or personnel enter or exit must 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 storage areas.

1.4 Building Structure

Buildings must be constructed of materials that resist unlawful entry.

The integrity of the structures must be maintained by periodic inspection and repair.

1.5 Locking Devices and Key Controls

All external and internal windows, doors, fences and gates must be secured with locking devices or alternative access monitoring or control measures.

Management or security personnel must control the issuance of all locks and keys.

1.6 Lighting

Adequate lighting must 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.

"must" denotes mandatory requirements

1.8 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.

1.9 Access Controls for Employees

An employee identification system must be in place for positive identification and access control purposes.

Employees should only be given access to those areas needed for the performance of their duties.

1.10 Access Controls for Visitors and Vendors / Contractors

A positive identification system must be in place to manage access control for visitors and vendors/ contractors.

All visitors should be escorted and visibly display identification passes.

1.11 Challenging and Removing Unauthorised Persons

Procedures must 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 employees. Procedures must be in place to create awareness for employees, on security and actions to be taken in response to security threats.

2.1. Pre-Employment Verification and Background Checks

Application information, such as employment history and references, must be verified prior to employment.

Background checks and investigation should be conducted on prospective employees as appropriate and to the extent allowed under national law.

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.

2.3. Security Awareness

A security awareness programme must be provided to relevant employees to recognise and foster awareness of security threats.

The security awareness programme should include the following:

- Recognising potential risks
- Maintaining cargo integrity
- Protecting access controls

Employees must be made aware of the procedures the company has in place to address a situation and how to report it.

2.4. Resignation and Termination of Personnel

Procedures must be in place to remove identification cards, as well as premises and information systems access for terminated and resigned employees.

"must" denotes mandatory requirements

3. Business Partner Security

Companies must work with business partners and obtain their commitment to voluntarily improve 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 must be in place for the screening and selection of business partners.

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

3.2. Security Requirements for Business Partners

Business partners must demonstrate that they are meeting the company’s supply chain security obligations in any of the following ways:

- through written or electronic confirmation;
- through contractual obligations;
- through a letter from a senior business partner officer attesting to compliance;
- through a written statement demonstrating their compliance with STP or other supply chain security programmes; or
- by providing a completed supply chain security profile.

3.3. Business Partners’ Participation/Certification in STP or Other Related Supply Chain Security Programmes

Company must have documentation indicating their business partners’ status of participation in the Secure Trade Partnership programme, supply chain security programme(s) administered by foreign Customs administrations or in other related supply chain security programme(s).

3.4. Review of Business Partners’ Compliance to Security Requirements

Procedures must be in place to monitor and review business partners’ compliance to security requirements.

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 persons.

4.1. Documentation Processing and Verification

Procedures must 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.

“must” denotes mandatory requirements

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 order 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 must 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 must 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:

- (h) Front wall;
- (i) Left side;
- (j) Right side;
- (k) Floor;
- (l) Ceiling;
- (m) Inside/outside doors; and
- (n) Outside/undercarriage.

4.5. Seals

Procedures must be in place on how seals are to be controlled, affixed and checked.

Only designated authorised person(s) should distribute seals.

For containers that are bound for the United States, the seals must meet or exceed the current PAS ISO 17712 standards for high security seals.¹

4.6. Storage of Containers and Cargo

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

5. Conveyance Security

Procedures must be in place to protect the conveyance (e.g. trucks, prime

¹ This may include shipments bound to countries that Singapore enters into a Mutual Recognition Arrangement (MRA) with and that the countries require the usage of high security seals.

“must” denotes mandatory requirements

movers, trailers) against the introduction of unauthorised personnel and material.

5.1. Conveyance Inspection

Procedures must be in place to ensure that potential places of concealment on conveyances are regularly inspected.

5.2. Tracking and Monitoring of Conveyance

Procedures must be in place to track and monitor the movement of conveyance carrying the cargo between companies and external parties.

5.3. Drivers' Guide

Guidelines should be in place to train drivers on:

- (g) Inspection of conveyance;
- (h) Confidentiality of load, route and destination;
- (i) Policy on keys, parking area, refuelling and unscheduled stops;
- (j) Reporting for accident or emergency;
- (k) Reporting of any irregularity in loading, locking and sealing; and
- (l) 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 and information systems used in the supply chain including protection against misuse and unauthorised alteration.

6.1. Information Security Procedures

Information security procedures and/or security related controls must be in place to protect information systems from unauthorised access.

6.2. Accountability

A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data.

6.3. 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

“must” denotes mandatory requirements

Procedures must be in place for reporting incidents to management. Incidents include short landing and over landing of cargo, irregularity or illegal activities and security breaches.

7.2. Investigate and Analyse

Procedures must 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 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 programme,
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 #07-01

Revenue House

Singapore 307987



Singapore Customs