SECURE TRADE PARTNERSHIP

SINGAPORE CUSTOMS

HANDBOOK

Preface

International trade is one of the key drivers of global economic growth. In today's globalised world, cargo supply chains are highly interconnected, complex and involve multiple players.

The ever-increasing complexity of the global supply chain also means more vulnerability to threats such as thefts, pilferages and terrorist attacks. It would be most unfortunate should the global trading system be disrupted by a single act of crime or terror anywhere along the supply chain.

Total supply chain security can only be achieved if every player along the entire supply chain, right from the point of origin to the point of final destination, takes responsibility in securing his part of the supply chain. To fulfil this objective, many countries have implemented or are implementing their national supply chain security initiatives.

As a key player in the global supply chain, Singapore has implemented the Secure Trade Partnership (STP) programme in partnership with our businesses to help raise the overall level of supply chain security standards in Singapore. The STP will ensure that we are not just an efficient and connected port, but also a safe and secure trading hub.

Contents

1 About This Handbook

1.1 Is this handbook meant for me?

1.1.1 If you wish to have your company certified under the Secure Trade Partnership (STP) programme, you should read this handbook.

1.2 What is this handbook about?

This handbook provides you with information on:

a) How the STP programme works; (Please refer to Section 2.)

b) The requirements under the STP Guidelines and Criteria; (Please refer to Section 3.)

c) How to apply for the STP; (Please refer to Section 4.)

d) What is a STP validation; (Please refer to Section 5.)

e) Certification under the STP; (Please refer to Section 6.) and

f) Other information. (Please refer to Section 7.)

2 Overview of the Secure Trade Partnership (STP)

2.1 What is the Secure Trade Partnership (STP)?

2.1.1 Launched on 25 May 2007, the STP is a voluntary certification programme administered by Singapore Customs to help companies adopt robust security measures to enhance the security of the global supply chain.

2.1.2 The 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. Companies meeting such requirements will be certified as STP companies by Singapore Customs.

2.1.3 The STP is consistent with the World Customs Organisation (WCO) SAFE Framework of Standards to secure and facilitate global trade, adopted in June 2005.

2.2 How does the Secure Trade Partnership (STP) work?

2.2.1 By participating in the STP, companies will be demonstrating their commitment to adopt and implement appropriate security measures and their willingness to assume responsibility for keeping their supply chains secure.

2.2.2 Companies that decide to apply for certification under the STP will first need to self-assess against the STP Guidelines and Criteria to ensure that their internal policies, processes and procedures are robust.

2.2.3 Singapore Customs administers a validation and certification process to certify companies that wish to participate in the STP.

2.2.4 Under the STP Guidelines and Criteria, companies are required to have security management systems, conduct risk assessments of their business operations, and implement the security measures that address the 8 elements under the STP Programme:

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.

Please refer to Section 3 for an Overview of the STP Guidelines and Criteria.

2.2.5 The STP certification will be valid for **up to** 3 years, depending on the result of the validation assessment. Certified companies must comply with the terms and conditions stipulated by Singapore Customs. Singapore Customs will conduct periodic and regular site visits. Please refer to Section 6 for more details on certification under the STP.

2.3 Who can apply for the Secure Trade Partnership (STP)?

2.3.1 The STP is open to companies in Singapore that are directly involved in the international supply chain activities. Companies which believe that they can meet the requirements under the STP Guidelines and Criteria can apply to join the STP.

2.3.2 In reviewing an application from a company, Singapore Customs will consider the following:

a) The company's compliance history with Singapore Customs and other relevant government authorities;

b) The company's security measures and standards; and

c) Related information on the company from local and/or foreign government authorities, where appropriate.

2.4 Why would a company want to be part of the Secure Trade Partnership (STP)?

2.4.1 A company that is certified under the STP will be recognised as a trusted partner of Singapore Customs and will partner Singapore Customs to enhance the security of the global supply chain.

2.5 What are the benefits of joining the Secure Trade Partnership (STP)?

2.5.1 Companies that have adopted and implemented robust security measures will benefit from increased visibility of goods in the supply chain, reduction in pilferages and greater efficiency in their supply chain management.

2.5.2 In addition, companies certified under the STP will be recognised as trusted partners of Singapore Customs and enjoy the following benefits:

a) Cargo less likely to be inspected domestically;

b) Recognition as a low risk company i.e. enhanced branding;

c) Recognised as a Known Consignor under the Regulated Air Cargo Agent Regime (RCAR); and

d) Reduced inspection or expedited clearance should the STP-Plus certification be recognised by overseas countries through Mutual Recognition Arrangement[1] (MRA).

2.6 Will the Secure Trade Partnership (STP) Guidelines and Criteria apply equally to companies of all sizes?

2.6.1 The STP recognises that business operation models, sizes and risks vary across the different nodes in the supply chain and across different industries and may therefore allow for flexibility and customisation of security measures based on companies' business models.

2.7 Will participation in other security programmes affect a company's obligation to comply with the requirements under the Secure Trade Partnership (STP) Guidelines and Criteria?

2.7.1 The STP recognises that companies may have already undertaken security measures on their own accord to strengthen their internal security systems, or may have already participated and implemented measures under other security programmes. It is not the intention of the STP to replace or supersede a company's existing security systems or measures. The STP seeks to build upon industry best practices and partnerships to strengthen the security of the global supply chain.

2.7.2 The various security programmes have slightly different objectives and hence, they will not be direct substitutes for the STP. Existing certifications that a company already complies with will be taken into account, if the security requirements are comparable to those required under the STP Guidelines and Criteria.

[1] For more information, please refer to **the Factsheet on Mutual Recognition**)

3 Overview of the Secure Trade Partnership (STP) Guidelines and Criteria

3.1 What are the Secure Trade Partnership (STP) Guidelines and Criteria?

3.1.1 The 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. Companies meeting such requirements will be certified as STP companies by Singapore Customs.

3.1.2 Under the STP Guidelines and Criteria, companies are required to:

a) Have security management systems;

b) Conduct risk assessments of their business operations;

c) Implement the stipulated security measures under the STP Guidelines and Criteria to secure their supply chains

d) Be part of the international supply chain, which can start from the manufacturing process to delivery of goods using the import and export procedures; and

e) Accountable and responsible of the cargo under their care.

3.1.3 The STP Guidelines and Criteria provides companies with a framework to guide the development, implementation, monitoring and review of their security measures and practices.

3.1.4 For more details, please refer to Annex A for the STP Guidelines and Criteria.

3.2 How do I know if I can meet the requirements?

3.2.1 Companies that wish to participate in the STP should note that there are two tiers - the STP certification and the STP-Plus certification. The different tiers have different requirements.

3.2.2 When a company wishes to obtain the STP or STP-Plus certification, the company has to go through Singapore Customs' Trade Facilitation & Integrated Risk-based System (TradeFIRST) assessment. Companies that that are able to meet all relevant mandatory criteria and attain at least the "Intermediate" banding would qualify for the STP certification; companies that are able to meet all relevant mandatory criteria and attain the "Premium" TradeFIRST banding would qualify for the STP-Plus certification.

3.2.3 Companies may refer to TradeFIRST dictionary in the TradeFIRST Self-

assessment checklist for the relevant mandatory criteria.

3.3 What is the security management system?

3.3.1 Supply chain security should be implemented holistically throughout the company, and not the sole responsibility of a person or a unit. Companies must establish security management systems to develop, document, implement, maintain and review their 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 continual relevance and improvement.

3.4 Why is the risk assessment process necessary?

3.4.1 The STP encourages companies to develop and implement security measures based upon risk assessments of their business models. Companies must conduct risk assessments of their operational processes and supply chains.

3.4.2 Companies must seek to mitigate the identified risks and vulnerabilities of their operations within the supply chains.

3.5 What are the security measures' requirements?

3.5.1 The security measures under the STP Guidelines and Criteria comprise 8 security elements that companies 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 recovery.

3.5.2 The security measures adopted or implemented must seek to mitigate the

risks and vulnerabilities identified from the company's risk assessment process.

3.5.3 For more details, please refer to Annex A for the STP Guidelines and Criteria.

4 Application for the Secure Trade Partnership (STP)

4.1 What information should be provided when a company applies for the Secure Trade Partnership (STP)?

4.1.1 The information to be submitted in a company's application should include:

a) An introduction of the company;

b) Application Form for the STP;

c) Accounting and Corporate Regulatory Authority (ACRA) Bizfile report;

d) Audited financial statements for the past 3 years;

e) Copy of the company's relevant security accreditations;

f) Completed TradeFIRST self-assessment checklist which includes relevant supporting documents attached as evidence for the "yes" responses;

g) Director's Declaration For Application of Schemes and Licences for the relevant personnel listed in the ACRA Bizfile report;

h) Security measures put in place by the company to enhance the security of the company's supply chain;

i) Process map(s) that illustrates the flow of goods and documentation/information through the company's supply chain. Please refer to Annex C for the Fact Sheet on Company's Process Map;

j) Site plan(s) that shows the layout of the company's premises and clearly identifies all perimeters, access areas, buildings, structures, security and access controls. Please refer to Annex D for the Fact Sheet on Company's Site Plan; and

(f) Any other relevant supporting documents as mentioned in the TradeFIRST self-assessment checklist.

Please refer to Customs website for more information.

4.2 What information should be provided for the introduction of a company?

4.2.1 The introduction of a company should contain the following information:

a) The background and history of the company;

b) The company's principal operations and supply chain operations that are outsourced to third parties;

c) Products that the company is dealing with;

d) The company's organisation chart and number of employees;

e) The company's relevant security accreditations; and

f) Any other relevant information.

4.3 What information should be provided for the summary of a company's management system?

4.3.1 The summary of a company's security management system should contain the following information:

a) The company's security policy, security objectives and commitment to security;

b) The procedures for ensuring that pertinent security management information is communicated to and from relevant employees and other stakeholders;

c) The procedures for the review of the company's security measures at planned intervals to ensure its continual suitability, adequacy and effectiveness; and

d) Any other relevant information.

4.4 What information should be provided for the summary of a company's risk assessment?

4.4.1 The summary of a company's risk assessment should contain the following information:

a) A flow chart to illustrate the company's risk assessment process;

b) The risks and vulnerabilities identified from the company's risk assessment process;

c) The countermeasures put in place to reduce the identified risks and vulnerabilities;

d) When the risk assessment was conducted;

e) Who conducted the risk assessment; and

f) Any other relevant information.

4.5 Does a company need to engage a consultant to assist in the conduct of the company's risk assessment?

4.5.1 It is not a requirement under the STP for a company to engage a consultant to assist in the company's risk assessment. It is the company's sole discretion whether to engage a consultant.

4.6 What is the level of detail to be provided in a company's application?

4.6.1 A company should provide as much information as possible in its application, making references to supporting documents such as standard operating procedures which can be attached together with the STP application. This will allow Singapore Customs to be more familiar with and obtain a better understanding of the security measures put in place by the company.

4.7 What if one of the security measures does not apply to my company?

4.7.1 The STP recognises the complexity of international supply chains and may allow for flexibility and customisation of security measures based on companies' business models as long as they are in line with international standards and practices. If one of the security measures does not apply to your company, please explain why. If your company adopts measures that are different from those in the STP Guidelines and Criteria, please document them in your application.

4.8 Can I use reference to describe my company's security measures?

4.8.1 Yes. You can use references such as standard operating procedures for the security measures, provided this is prefaced with a short description. The standard operating procedures can be attached together with the STP application.

4.9 Do I need to cover all sites in my company's application for STP?

4.9.1 Yes, all your company's sites will be covered in the STP application. Where operations at any of these sites are considerably different, your company should develop separate assessments and state the security measures put in place for each type of operation.

4.10 Are there terms and conditions for application to the Secure Trade Partnership (STP)?

4.10.1 Yes, please read the terms and conditions stipulated in the online application form for the STP.

4.11 Do I need to submit security write-up of my company's business partners?

4.11.1 Yes, you should provide information/documents related to the elements of your company's supply chain that are outsourced or contracted to your business partner. The officer who is processing the application will advise on the information/documents requirements, where appropriate.

4.12 How do I apply?

4.12.1 To apply for the STP, please send your completed STP application **here**, complete the **TradeFIRST Self-Assessment Checklist** and relevant annexes, and attach soft copies of relevant supporting documents to Singapore Customs via e-mail to customs_schemes@customs.gov.sg

4.13 How long will the application process take?

4.13.1 In general, the application process will take about 5 months but it may take a longer time depending on the completeness of information/documents submitted to Singapore Customs, the complexity of a company's business operations and the number of sites to be assessed. The officer processing the company's application will be able to provide an indication of the timeframe.

4.14 How much will the application cost?

4.14.1 There is no application fee.

5 Validation

5.1 What is a validation under the Secure Trade Partnership (STP)?

5.1.1 A validation is a process by which Singapore Customs visits a company to verify that the information outlined in the company's application is accurate and implemented.

5.1.2 The validation visit also serves as a platform for Singapore Customs and the company to build up a partnership of trust and to develop a better understanding of each other.

5.2 Will all companies that decide to participate in the Secure Trade Partnership (STP) undergo a validation?

5.2.1 Yes, all companies that decide to participate in the STP will have to be validated by Singapore Customs before they are certified.

5.3 Who will conduct the validation?

5.3.1 Singapore Customs will conduct the validation.

5.4 What is expected of a company during a validation?

5.4.1 The company must have all relevant documents/information available for review during the validation. The company must arrange for a tour of the company's site(s) and have company representatives available during the validation to address the company's security measures under the following 8 security elements:

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 recovery.

5.5 Will Singapore Customs conduct validations at all the company's sites?

5.5.1 Yes, Singapore Customs will conduct validations at all the company's sites.

5.6 Will Singapore Customs conduct validation on a company's business partners?

5.6.1 Singapore Customs may conduct selective validations on the company's key business partners. The officer who processes the company's STP application will advise on the validation requirements, where appropriate.

5.7 Will Singapore Customs conduct overseas validation?

5.7.1 Singapore Customs will not conduct overseas validation.

5.8 How will validation findings impact a company's participation in the Secure Trade Partnership (STP)?

5.8.1 Depending on the certification applied for, the company will be granted either the STP certification or STP-Plus certification if it attains the relevant TradeFIRST banding and meets all relevant mandatory criteria.

5.8.2 If the validation findings reveal significant weaknesses in the company's security measures, Singapore Customs will reject the application or work with the company to develop an action plan to close the gaps before re-submitting its application for Singapore Customs' re-assessment and validation.

5.9 Will validation findings be communicated to the company?

5.9.1 Yes, Singapore Customs will communicate the validation findings to the company.

5.10 How long will the validation process take?

5.10.1 The duration of the validation process will depend on the completeness of information/documents submitted to Singapore Customs, the complexity of a company's business operations and the number of sites that the company has. The officer who processes the company's application will be able to provide an indication of the timeframe.

6 Certification under the Secure Trade Partnership (STP)

6.1 What are the responsibilities of a Secure Trade Partnership (STP) company?

6.1.1 In addition to the responsibilities stated in the Application Form, a STP company's responsibilities include:

a) To update Singapore Customs as and when there are significant changes to the company's security measures;

b) To notify Singapore Customs of all changes to the company's information including company's name, corporate address, contact number, website address, company's point of contact, principal operations and relevant accreditations; and

c) To inform Singapore Customs of any non-conformities by the company in relation to the STP Guidelines and Criteria.

More information can be found in the relevant terms and conditions issued to a successful applicant.

6.2 Can my STP or STP-Plus certification be extended to my customer's warehouse operated by my company?

6.2.1 No, the STP or STP-Plus certification is only applicable for premises owned/leased by your company.

6.3 Will Singapore Customs conduct site visits to an STP company during the certification period?

6.3.1 Yes, Singapore Customs may conduct periodic and regular site visits. Singapore Customs will provide notice to the STP company prior to the site visits.

6.4 Will there be any penalties imposed on an STP company for non-compliance to the terms and conditions?

6.4.1 Non-compliance to the terms and conditions of the STP certification will result in suspension or removal of a company's certification and associated benefits.

6.5 When will a company's STP or STP-Plus certification be suspended?

6.5.1 A company can have its STP or STP-Plus certification suspended if:

a) The company does not abide by the terms and conditions of the certification; or

b) There is non-compliance by the company with Singapore Customs laws and regulations and/or with the laws and regulations of other relevant Singapore government authorities; or

c) Supply chain security weaknesses in the company or non-conformity by the company with STP Guidelines and Criteria are discovered and not addressed to Singapore Customs' satisfaction.

6.5.2 Once suspended, the company will lose its certification and associated benefits and they will only be re-instated if the company addresses the areas of weakness or non-compliance to the satisfaction of Singapore Customs.

6.5.3 If the company is unable to take the required measures to address the areas of weakness or non-compliance to the satisfaction of Singapore Customs within a stipulated period of time, the company will have its STP certification revoked and associated benefits removed.

6.6 When will a company's STP or STP-Plus certification be revoked?

6.6.1 A company can have its STP or STP-Plus certification revoked if:

a) The company does not abide by the terms and conditions of the certification and has not taken sufficient measures to correct these non-compliance despite given sufficient notice by Singapore Customs to do so; or

b) There is serious non-compliance by the company with Singapore Customs laws and regulations and/or with the laws and regulations of other relevant Singapore government authorities; or

c) Serious supply chain security weaknesses in the company or non-conformity by the company with STP Guidelines and Criteria are discovered and not addressed to Singapore Customs' satisfaction.

6.6.2 Once the certification is revoked, any associated benefits accorded to the company, will be removed immediately.

6.6.3 After the revocation, the company can only re-apply for STP certification after 1 year from the date of revocation.

6.7 Can a STP company withdraw from the Secure Trade Partnership (STP)?

6.7.1 Yes, the STP is a voluntary programme and a STP company is able to withdraw from the STP if it no longer wishes to be in the programme. The company has to write in to inform Singapore Customs of its withdrawal. Upon withdrawal, the company will have its STP or STP-Plus certification and associated benefits removed.

6.8 Can a company's STP or STP-Plus certification be renewed?

6.8.1 Yes, a company can renew its STP or STP-Plus certification if it wishes to continue to participate in the STP. The renewal process is the same as the application process. Please refer to Section 4 of this handbook.

7 Other Information

7.1 Who will have access to business documents/information provided in companies' applications?

7.1.1 The business documents/information are for Singapore Customs' purposes only and will not be disclosed to a third party without the companies' prior written consent. All business documents/information provided by the companies will remain confidential.

7.2 Is there an appeal process within the STP programme?

7.2.1 A company can appeal against a decision made by Singapore Customs with regard to the company's application and participation in the STP programme. The company has to lodge its written appeal with Singapore Customs within 28 days from the date of the relevant decision communicated to the company by Singapore Customs.

7.3 Contact information

7.3.1 This handbook is developed to provide a general overview of the STP programme. Should you need further clarifications or advice, please e-mail customs_schemes@customs.gov.sg

Annex A

STP Guidelines and Criteria

A Security Management System

1. Supply chain security should be implemented holistically throughout the company, and not the sole responsibility of a person or a unit operating within a company.

2. The 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 continual relevance and improvement.

B Risk Assessment

1. The STP encourages companies to develop and implement security measures based upon a risk assessment of the companies' business models.

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

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 beginning so as to minimise exploitable data errors or the need for content verification at later stages in the chain. With accurate manifests and documented handing-over processes, and tamper-proof packaging, manufacturers and suppliers will be able to hand over their goods to the cargo handling agents, such as warehouse operators and transport companies, for them to be moved through the supply chain securely.

Warehouse Operators and Owners

Warehouse operators and owners receive goods from manufacturers, transporters or other intermediaries, store them, and in turn hand 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 entrusted to them are safe from tampering.

Transporters

Transport operators have a key responsibility in ferrying goods from one point to another. Transport operators should have measures in place 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 carried by their vehicles are not easily tampered with.

Terminal Operators

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 entrusted to them are safe from tampering.

Sea and Air Freight Operators

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 in place to prevent their carriers from being hijacked or substituted while en-route to their destination. They should have a good information system to monitor and track the goods entrusted to them. In addition, sea and air freight operators should ensure that their vessels and aircrafts and goods carried on board their vessels and aircrafts are not easily tampered with.

C 8 Security Elements

"must" denotes mandatory requirements for STP-Plus

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 the 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 the 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, access cards and keys.

1.6 Lighting

Adequate lighting must be provided inside and outside the 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 enter the premises, 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 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, and 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 investigations should be conducted on prospective employees as appropriate, and to the extent allowed under national laws.

2.2. Periodic Background Checks / Re-investigations for Current Employees

Periodic checks and re-investigations 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 employees whose services have been terminated, or have resigned.

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 write-up.

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 and protected 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.

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/or Stamp Policies

Procedures should be in place on signature and/or 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:

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 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.[2]

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 movers, trailers) against the introduction of unauthorised personnel and

[2] 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.

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:

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 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

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.

Annex B

Mandatory Criteria to Qualify for STP and STP-Plus

The mandatory criteria to qualify for the STP-Plus certification are stipulated in the TradeFIRST self-assessment checklist. Please see the table below for the correlation of the STP Guidelines and Criteria and the TradeFIRST self-assessment checklist.

STP Guidelines and Criteria		**Mandatory STP Criteria under TradeFIRST***	
1.5	Locking devices and key controls	11F	Locking devices and key controls
1.9	Access Controls for Employees	11K	Employee identification
2.1	Pre-Employment Verification and Background Checks	3A	Pre-Employment Verification and Background Checks
4.1	Documentation Processing and Verification	2C	Permit Declaration
		5A	Data Integrity/Accuracy
6.1	Information Security Procedures	2B	System Security

* companies are still highly encouraged to fulfil the other criteria in the TradeFIRST checklist in order to meet the minimum “Intermediate” banding.

STP Guidelines and Criteria		**Mandatory STP–Plus Criteria under TradeFIRST**	
1.1	Perimeter fencing	11G	Internal Demarcation
		11B	Perimeter Fencing
1.2	Gates and Gate Houses	11C	Positive Identification for Visitors, Contractors & Drivers
1.3	Parking	11E	Parking
1.5	Locking devices and key controls	11F	Locking devices and key controls
1.6	Lighting	11H	Lighting at critical areas
1.7	Alarm Systems and Video Surveillance Cameras	11I	Alarm Systems
		11J	Video Surveillance Cameras
1.8	Security Personnel and Organisation	11A	Security Personnel
1.9	Access Controls for Employees	11K	Employee identification
1.10	Access Controls for Visitors and Vendors/ Contractors	11C	Positive identification for Visitors, Contractors & Drivers
1.11	Challenging and Removing Unauthorised Persons	11L	Challenging and Removing Unauthorised Persons
2.1	Pre-Employment Verification and Background Checks	3A	Pre-Employment Verification and Background Checks
2.2	Periodic Background Checks for Current Employees	3B	Periodic Background Checks for Current Employees
2.3	Security Awareness	4C	Security Awareness Training
		4A	Customs Procedures Training
2.4	Resignation and Termination of Personnel	3C	Resignation and Termination of Personnel
3.1	Screening of Business Partners	6A	Screening Procedures

STP Guidelines and Criteria		Mandatory STP–Plus Criteria under TradeFIRST	
3.2	Security Requirements for Business Partners	6B	Security Requirements
3.3.	Business Partners' Participation/Certification in STP or Other Related Supply Chain Security Programmes		
3.4	Review of Business Partners' Compliance to Security Requirements	6A	Screening Procedures
4.1	Documentation Processing and Verification	2C	Permit Declaration
		5A	Data Integrity/Accuracy
4.2	Receipt and Release of Cargo	10A	Cargo Receiving
		10B	Cargo Releasing
4.3	Signature and/or Stamp Policies	10A	Cargo Receiving
		10B	Cargo Releasing
4.4	Container Inspection	8A	Container Inspection & Storage
4.5	Seals	8B	Container seals management
		8C	Container seals types
4.6	Storage of Containers or Cargo	9A	Conveyance Storage & Inspection
5.1	Conveyance Inspection	9A	Conveyance Storage & Inspection
5.2	Tracking and Monitoring of Conveyance	9B	Tracking and Monitoring of Conveyance
5.3	Drivers' Guide	9C	Drivers' Guide
5.4	Storage of Conveyance	9A	Conveyance Storage & Inspection
6.1	Information Security Procedures	2A	Information Management
6.1	Information Security Procedures	2B	System Security
6.2	Accountability	2A	Information Management
6.3	Data Back-ups and Recovery Plans		
7.1	Reporting Incidents	7B	Incident Handling & Reporting
7.2	Investigation and Analysis		
8.1	Contingency or Emergency Plans	7C	Contingency or Emergency Plans
8.2	Business Continuity Plan (BCP)	7D	Business Continuity Plan (BCP)

Annex C

Fact Sheet on Company's Process Map

1 What is a process map?

1.1 A process map illustrates the flow of goods and documentation/information through a company's supply chain.

2 Why is the process map necessary?

2.1 The process map allows Singapore Customs to see the continuous link of activities that take place within a company's supply chain and provides us with a better understanding of the company's entire supply chain.

3 What information must the process map contain?

3.1 The process map must cover a company's entire supply chain, accounting for both the physical and documentary processes.

4 What if a company has multiple sites with different operations?

4.1 If a company has multiple sites and operations at any of these sites are considerably different, the company should develop separate process maps for each type of operation.

5 If a company has many different products that undergo different logistics routes and supply chain processes (i.e. process maps), does the company need to provide a process map for each product?

5.1 If there are many different supply chain processes, a company can provide a general process map that shows the different activities involved at each stage. Singapore Customs will request for detailed process maps, if necessary. If a general process map is not feasible, the processes should be separately mapped.

5.2 An example of a basic process map is attached to assist you.

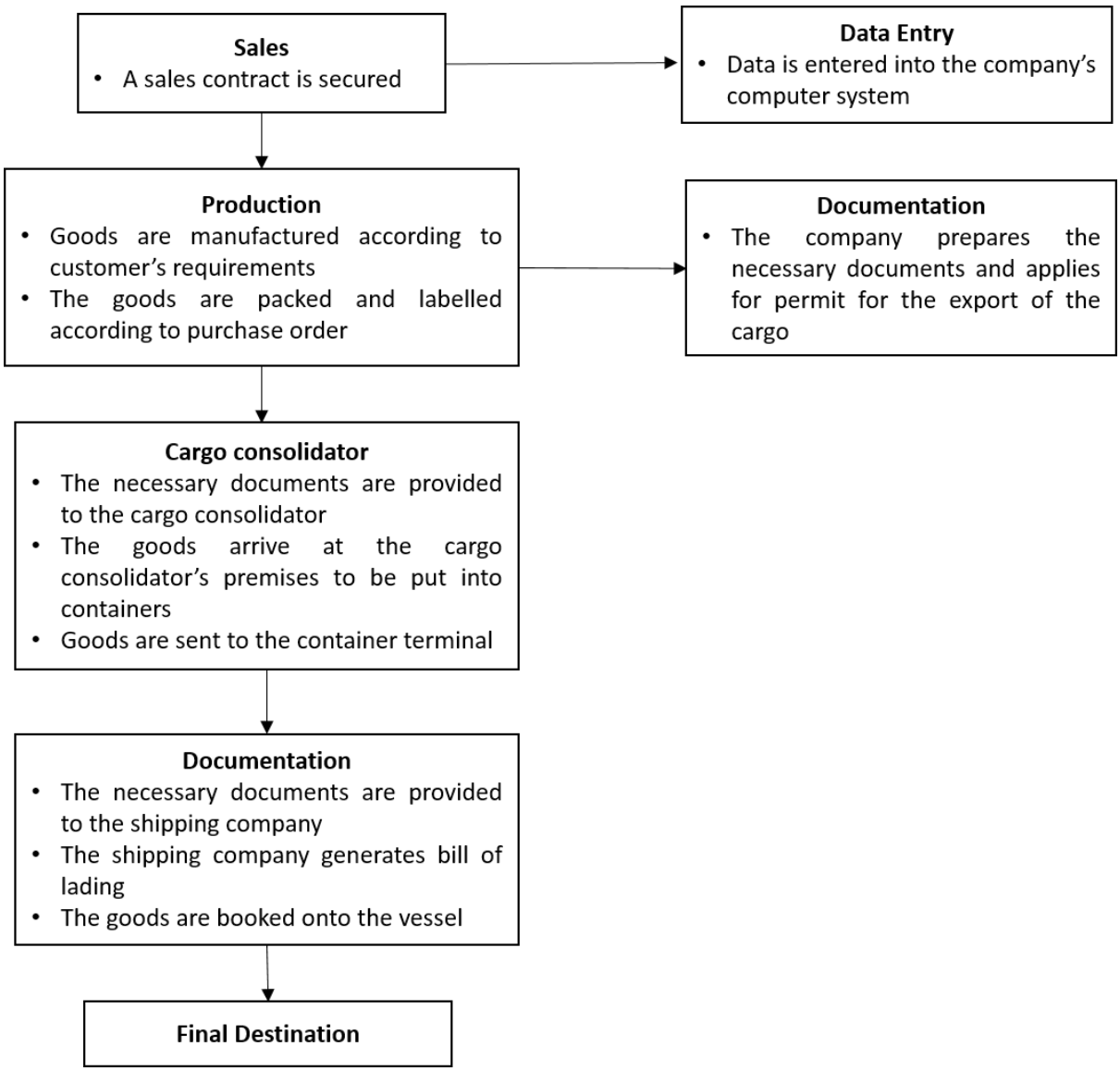
An Example of a Process Map

Name of company:

Dated:

Name of site:

Type of operation:



Annex D

Fact Sheet on Company's Site Plan

1 What is a site plan?

1.1 A site plan shows the layout of a company's premises and clearly identifies all perimeters, access areas, buildings, structures, security and access controls.

2 Why is the site plan necessary?

2.1 The site plan provides Singapore Customs with an overview of the environment where a company operates and the security features on-site to enhance the security of the company's operations.

3 What information must the site plan contain? How detailed must the site plan be?

3.1 The site plan must be to scale and clearly identify a company's site boundaries, the various buildings within the site and also the usage of any open areas. Entry points to the site and the buildings within the site must be clearly indicated and labeled. The company should also preferably include in the site plan the positions of lightings (flood lights, emergency lights etc.), CCTVs (coverage) and any other security equipment in the company's premises. The site plan must be dated and identified with the name and address of the site.

4 What if a company has multiple sites?

4.1 If a company has multiple sites and the layouts at any of these sites are considerably different, the company should develop separate site plans for each site.

Contact Us

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

Schemes & Engagement Branch
Singapore Customs
55 Newton Road #06-01
Revenue House
Singapore 307987

SINGAPORE CUSTOMS