



Tel: 519-326-0101 Fax: 519-326-0204  
www.bonneaufreight.com

# CLIENT SECURITY QUESTIONNAIRE

## COMPANY INFORMATION

LEGAL NAME OF COMPANY	
TRADE NAME (if different than above)	

	PHYSICAL ADDRESS	MAILING	<input type="checkbox"/> Same as physical address
STREET:			
CITY, PROV.			
POSTAL CODE			
NAME:		TITLE:	
PHONE:		FAX:	
E-MAIL:		WEBSITE:	

## CERTIFICATIONS

Please specify your participation in any Canadian or US Customs Partnership programs and attach certificates where applicable:

	YES	NO	APPLICATION IN PROGRESS	ESTIMATED DATE OF APPROVAL	NO PLANS TO APPLY
FAST					
CSA					
PIP					
C-TPAT					

If C-TPAT certified, please e-mail your SVI to [admin@bonneaufreight.com](mailto:admin@bonneaufreight.com) through the CBP portal.

## SECURITY QUESTIONS

Do you have documented Security Procedures in place that are comparable to the attached Security Recommendations?

	SECTION	YES	NO
1.	Business Partners Requirements		
2.	Conveyance/Container Security		
3.	Physical Access Controls		
4.	Personnel Security		
5.	Procedural Security		
6.	Physical Security		
7.	Security Training and Threat Awareness		
8.	Information and Technology Security		

AUTHORIZED PERSON: \_\_\_\_\_  
(SIGNATURE) (PRINTED NAME / TITLE) (DATE)



# **CLIENT SECURITY QUESTIONNAIRE**

## **Business Partner Requirements**

Importers must have written and verifiable processes for the selection of business partners including manufacturers, product suppliers and vendors. Screening procedures for new customers must go beyond financial soundness issues to include security indicators, such as business references and professional associations.

## **Conveyance/Container Security**

Conveyance/Container integrity procedures must be maintained to protect against the introduction of unauthorized personnel and material. Procedures should be in place to properly seal and maintain the integrity of shipping containers, verify the physical integrity of the container structure prior to stuffing and store containers in a secure area.

## **Physical Access Controls**

Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry. Employees and service providers should only have access to those areas of a facility where they have legitimate business.

## **Personnel Security**

Written and verifiable processes must be in place to screen prospective employees and to periodically check current employees including:

- Pre-Employment Verification
- Background Checks/Investigations
- Personnel Termination Procedures

## **Procedural Security**

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain. Procedures must be in place to ensure that all information used in the clearing of merchandise/cargo, is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information. All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately.

## **Physical Security**

Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access. Physical barriers include, fencing, alarms, gates, adequate lighting, secure access and segregated parking.

## **Security Training and Threat Awareness**

A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists at each point in the supply chain. Employees must be made aware of the procedures the company has in place to address a situation and how to report it. Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail.

## **Information & Technology Security**

Measures should be taken to protect electronic assets, including advising employees of the need to protect passwords and computer access. A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data.