



PENROD

SEA CARRIERS

These general questions should be answered on a case-by-case basis depending on the company's size and structure.

Business Partner Requirements: Sea carriers must have written and verifiable procedures for the screening of carrier's agents and service providers contracted to provide transportation services for the carrier.

Describe the review process used to determine that your business partners have adequate security measures in place to protect the integrity of the supply chain.

Container Security: Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons.

How are empty and full containers stored to prevent unauthorized access?

Describe the procedure for recognizing and reporting compromised seals and/or containers.

Physical Access Controls: The sea carrier shall establish access controls to prevent unauthorized entry to its vessels and cargo facilities, maintain control of employees and visitors, and protect company assets.

Describe how all employees, visitors, and vendors are identified prior to entering the container storage facility.

Describe the procedures in place to identify, challenge and address unauthorized/unidentified persons.

Personnel Security: Processes must be in place to screen prospective employees and to periodically check current employees.

What process does the company have for employment screening, application verifications, interviewing of prospective employees and periodic background checks?

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.

Describe the procedures in place for verifying seals on loaded containers.

What are the procedures for notifying Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected, or suspected, by the company?

Security Training and Awareness: A security awareness program should be established and maintained by the carrier to recognize and foster awareness of security vulnerabilities to vessels and maritime cargo.

What security awareness programs are provided to employees to include recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access?

Physical Security: Carriers must establish written and verifiable procedures to prevent unauthorized personnel from gaining access to its vessels, including concealment in containers, and to prevent tampering with cargo conveyances while they are in the carrier's custody.

Describe how container facilities are designed to resist unlawful entry and protect against outside intrusion.

Information Technology Security: Information Technology policies, procedures and standards must be in place and provided to employees in the form of training.

Is a system in place to identify the abuse of information technology including improper access, tampering or the altering of business data?

C-TPAT Compliance:

Are you eligible for C-TPAT Certification?

Yes No Not applicable

Have you applied for certification? If yes, have you received your certification? Please provide us with a copy of your C-TPAT Status Verification Interface number (SVI).

Other Security Accredited Organizations:

Does your company participate in other programs designed to certify supply chain security?

Yes No

If yes, please provide the name and contact information of these organization(s) and advise your level of participation. If you have received any certification from these organizations, kindly provide documents that reflect your certification.

Signature:

Company Name and Address:

Manager Name:

Manager Signature:

Date:

After the form is completed, kindly return via fax or PDF to your Penrod representative. Please note that we must have an actual signature.