

## **C-TPAT SECURITY REQUIREMENTS**

**1 BUSINESS PARTNER SECURITY:** After the incident of September 11, 2001 the whole world has taken actions to counter terrorism. All the security routines are modified to ensure their effectiveness and relevance, this program will continue to evolve and work in partnership with the stake holders of international supply chains- as the terrorist threat and the nature of global trade evolves.

**2 CONTAINER SECURITY:** Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At point of stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers. A high security seal must be affixed to all loaded containers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals.

**3 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.

**4 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.

**5 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 all area

**6 PHYSICAL SECURITY:** Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access. Importers should incorporate the following C-TPAT physical security criteria throughout their supply chains as applicable.

### **7 Information Technology Security - Password Protection:**

Automated systems must use individually assigned accounts that require a periodic change of password. IT officer change password of each computer after 60 days. IT security policies, procedures and standards must be in place and provided to employees in the form of training. A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data. All system violators must be subject to appropriate disciplinary actions for abuse.

## **8 PERSONNEL SECURITY**

The company should conduct employment screening and interviewing of prospective employees, the past job experience, references, address, contact numbers, identity card etc should be verified.

Ensure that no drug addict or a person with criminal background is inducted in service.

The background investigation may be initiated for every prospective employees

The company drivers must be checked for driving record background.

Periodical vetting may be initiated for employees work in vital departments/ areas.

Drug tests for suspected drug addict employees, must be initiated, periodically.

Termination procedures should be strictly followed, when a person is terminated from service.

**For Keep Update your facility please regularly visit C-TPAT / SCS official website**

**Company/ Supplier Name:** \_\_\_\_\_

**Signed & Stamp By:** \_\_\_\_\_