



**C-TPAT standard principles**



**IPQ Tecnologie srl**  
*Partner per lo sviluppo d'impresa*  
**Raffaella Vitiello**



# INTRODUCTION

- C-TPAT is an acronym for *Customs-Trade Partnership Against Terrorism*
- C-TPAT is a voluntary program offered by the U.S. Government
- C-TPAT requires employees to:
  - Advocate for adherence-wear your badge, secure your work location, remind others to ensure they comply;
  - Awareness – be alert for suspicious activity;
  - Reporting – all suspicious activity must be reported.



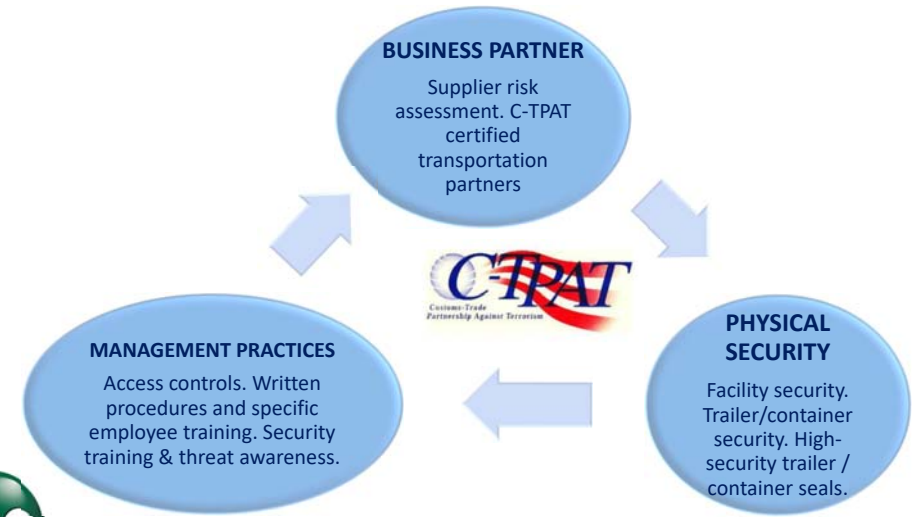
# RATIONALE

Being a trusted partner with U.S. Customs provides operational and financial benefits to Static Control such as:

- Fast lane processing for imports and exports
- Lower targeting score = less supply chain disruption due to Customs inspections
- Mitigation of fines and penalties in case of a Customs violation
- Brand protection and competitive advantages.



# MAJOR AREAS OF C-TPAT



## TOPICS

- Suspicious persons
- Suspicious activities
- Suspicious objects and packages
- Employee identification
- Visitor controls
- Computer security
- Document security



## SUSPICIOUS PERSONS

Any person:

- unescorted and without an employee badge, or visitor sticker, especially in an unauthorized / restricted area
- wearing unusual clothing such as an overcoat on a 95 degree day
- waiting or loitering in an area of hallway
- tampering with someone's desk, equipment, vehicles, camera, etc.
- running, especially if carrying something
- hiding behind doors, fences, desks, etc.



## SUSPICIOUS PERSONS

How to act...

- Challenge the person: ask if you can help them
- Determine if the person is an employee or a visitor:
  - if an **employee**, remind them always to display their ID badge
  - If a **visitor**, get them out of the restricted area and escort them to the reception area or to the person with whom they are visiting.
- Report the incident to your immediate supervisor.



## SUSPICIOUS ACTIVITIES

What to look for...

- Objects obstructing access points
- Cameras being disconnected or obstructed
- Broken locks or access control system
- Objects thrown from a vehicle, especially while traveling at high speeds



# SUSPICIOUS ACTIVITIES

How to act...

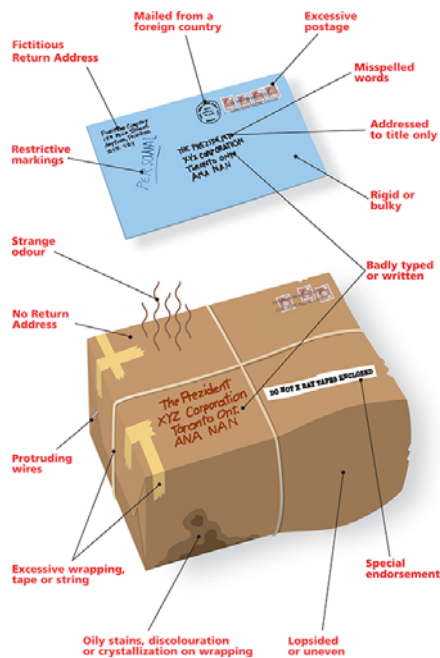
Immediately report any suspicious activity to your supervisor, so they can address the situation and cal security, if necessary.



# SUSPICIOUS OBJECTS OR PACKAGES

What to look for...

- Unexplained objects or packages that look strange or do not belong to the area
- Strange marking on boxes (unknown code, color) or strange characteristics (weight, number, odd shape)
- Strange leaking substance (powder, liquid, etc.)
- Suspicious objects in the middle of an area (e.g. hallway, lobby, etc.)



# SUSPICIOUS OBJECTS OR PACKAGES

How to act...

- Immediately report any suspicious packages or objects to your supervisor, security, local police.
- Handle with care, do not shake or bump
- Isolate and look for indicators (shape, color, smell)
- Do not open, smell, lick or taste
- Treat is as suspect



## EMPLOYEE IDENTIFICATION

Your responsibilities while on company property:

- Your static control components ID/security badge must be properly displayed and worn at all times
- Properly secure and protect your ID/security badge



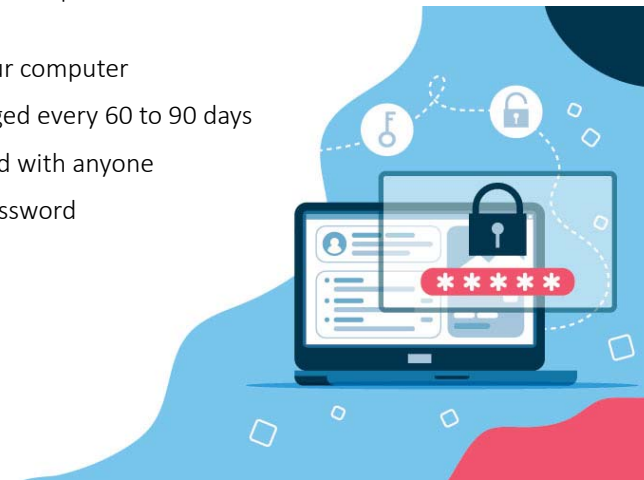
## VISITOR CONTROLS

- Pre-meeting requirements: inform your visitor of the company's visitor policies including the required photo identification, and check-in with receptionist prior to their visit
- Entrance requirements: ensure that your visitor has logged in and has been issued a visitor badge
- Escort requirements: you must escort your visitors at all times. Do not leave your visitor unattended
- Exit requirements: ensure that your visitor has logged out and has returned the visitor badge to the guard or receptionist.



## COMPUTER SECURITY

- Do not share access to your computer with strangers
- Log-off when you leave your computer
- Passwords should be changed every 60 to 90 days
- Do not share your password with anyone
- Do not write down your password



## COMPUTER SECURITY

Selecting a password:

- Use hard-to-guess passwords
- Do not use the same password in more than one place
- A password should have a mix of letters, numbers and symbols



# DOCUMENT SECURITY

- Follow all SOP documentation regulations
- Do not leave sensitive documents laying around, especially when you are away from your desk
- Once finished with sensitive documents, either file in a secure location (such as a locked room or filing cabinet), or shred the documents in a predetermined area

