MINIMUM SECURITY CRITERIA FOR BUSINESS PARTNERS

As part of the Customs-Trade Partnership Against Terrorism (C-TPAT) program, Reliant Customs Broker is committed to support the C-TPAT initiative amongst its business partners. There are certain practices that are recommended to avoid and safeguard our facilities and systems from terrorist actions.

About six months ago we requested your company to comply with the security measures to determine their compliance with our security requirements.

We are kindly requesting to review again our suggested Best Practices and to sign and send a copy back to us indicating you have received our request.

1. Partner Commitment to security

   a) Partner should have a designated Point of contact to supervise and maintain program

   b) Employees Should be trained on how to react to a breach of security incident

2. Risk Assessment

   a) Conduct risk assessment identifying vulnerabilities

   b) Identify threats and incorporate measurements to mitigate breach of security

   c) Written procedures to manage crisis, recovery plans and resume business

3. Business Partners Selection

   a) Written business process in place for screening new business partners

   b) Written business process to monitor current business partners

   c) Monitor activity related to money laundering

   d) Participation on a Security Program such as CTPAT

4. Information Technology and Cyber Security

a) Computer Server Area should be secured with access only to one or two authorized persons.

b) Computer systems should be protected by a firewall and Anti-virus software.

c) Internet and E-mail Use policies should be in place for employees.

d) Plan of corrective actions if vulnerabilities found

e) System should be in place to report and discipline unauthorized use or abuse of technology

5. Transportation Security

a) Conveyances and containers should be stored in safe areas

b) Written procedures should be in place for the inspection of containers

c) Transportation companies participating in security programs are preferred

d) Searches of conveyances should be conducted periodically

e) Written procedures to issue and control seals should exist

6. Procedural Security & Shipping and Receiving

a) Procedures should be in place to ensure data is complete and without compromise

a) Shipping and Receiving areas should be restricted allowing only authorized personnel

b) Drivers should show proof of identification and should be registered in a Visitor's log.

c) Container and seals should be inspected and identify against documentation.

d) Data and documentation should be restricted to only those employees authorized to handle administrative information.

7. Facility-Physical Security

    a) Partner's facilities should be guarded from unauthorized access

    b) Written Visitors Policy and Controls

    c) Security ID badge for all employees (for companies with 50 employees or more)

    d) Written Procedures for the removal of unauthorized persons

    e) Alarm System and procedures for invasion emergencies

    f) Locking devices in all doors and windows

8. Personnel Security

    a) Written Procedures in place for the screening of potential and current employees

    b) Employee background checks and periodical drug testing

    c) Code of Conduct that defines acceptable behaviors and disciplinary actions

9. Training and Security Awareness

    a) Training and Security Awareness Program should be in place.

    b) Routine Security Audits should be performed.

    c) Employee participation should be encouraged

    b) Active Corrections should be taken.

Please acknowledge of receipt and sign as a commitment to abide to Reliant's requirements to comply with the C-TPAT minimum security criteria.

_____

Company Name

_____

Name, Signature and Title:

_____

Date