Airline Security

0796- Airline Security Procedures

Revision Date: 05/13/19

Applicability

The following security training consist of security topics and must be completed by all UPS and Authorized Representative employee's working at regulated locations which include UPS Gateways, Last Look Air Recoveries (LLAR) and Cargo Handling Facilities (CHF).

Training must be documented in LMS using training code 0796. Training records must be made available for audit and inspection purposes. UPS must have a control in place which identifies when initial and annual/recurrent (+/- one month of initial training) training is due.

The following topics are covered in the Airline Security Procedures training:

1. Sensitive Security Information (SSI)
2. Fraud and Intentional Falsification of Records
3. Confidential Information
4. ID Media Display
5. Challenge Procedures
6. Reporting Suspicious Activities
7. Insider Threat Awareness (*new*)
8. Individual Accountability

Sensitive Security Information (SSI)

SSI is information obtained or developed which, if released publicly, would be detrimental to transportation security. SSI must be controlled regardless of its format or location.

This record contains SSI that is controlled under 49 CFR PARTS 15 AND 1520. UPS employees and Authorized Representatives must not disseminate SSI material related to security procedures to anyone unless there is a "Need to Know" except with the written permission of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action.

Fraud and Intentional Falsification of Records

No person may make, or cause to be made, any of the following:

- Any fraudulent or intentionally false statement in any application for any security program, access media, or identification media, or any amendment
- Any fraudulent or intentionally false entry in any record or report that is kept, made, or used to show compliance
- Any reproduction or alteration, for fraudulent purpose, of any report, record, security program, access media, or identification media issued

Original Date: 12/10/07

Airline Security

0796- Airline Security Procedures

Revision Date: 05/13/19

We Safeguard Confidential Information of Our Business Partners

We understand the importance of properly protecting the confidential information of our business partners, including customers, suppliers, and other third parties with whom we do business. We have an obligation to handle confidential information appropriately, using it only for business purposes and as authorized, according to any legal standards, agreements, or contractual provisions. We should follow appropriate UPS policies and procedures that address our responsibilities concerning such information.

ID Media Display

All individuals working in regulated areas must display approved ID Media **AT ALL TIMES**. All UPS employees and Authorized Representative employees must adhere to this important regulation by following the steps listed below:

- ID media must be worn above the waist and on the outer-most garment
- Never allow any individual or vehicle to piggyback (follow you through an access point)
- Never allow another individual to borrow your ID media
- Your ID media is unique and only valid for unescorted access to the regulated location identified on it
- Immediately report lost or stolen ID media to your management team and/or Security
- No individual should tamper or interfere with any security system, measure or procedure
- No individual shall duplicate their ID media nor shall they allow another individual to duplicate their ID media for any reason. This includes any request to duplicate from the Transportation Security Administration (TSA) or any other government agency.

Challenge Procedures

The TSA conducts inspections of our regulated locations to ensure we are carrying out challenge procedures around aircraft and cargo. UPS and Authorized Representative employees must carry out challenge procedures in order to prevent unauthorized access by unauthorized individuals. The challenge program UPS uses is referred to as **"iChallenge"**.
A proper challenge consists of the following three steps:

Participate, Communicate, and Eliminate

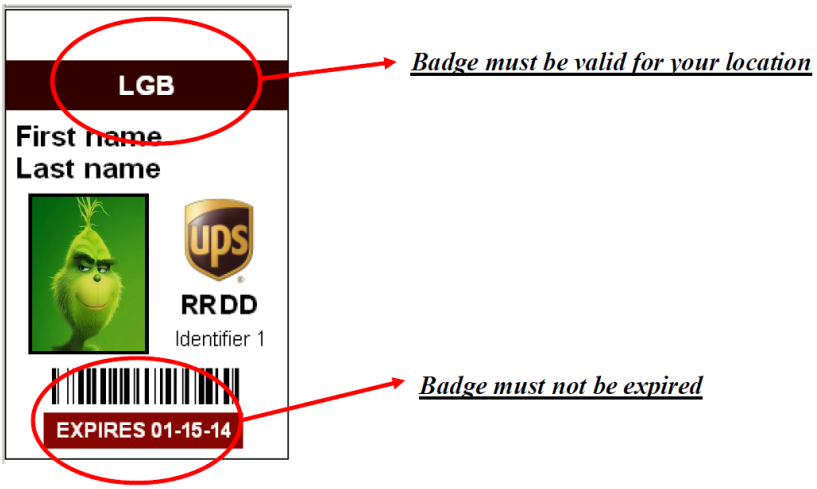
Participate

- When you spot an unknown and/or unbadged individual, approach the person

Communicate

- Offer a greeting like, "may I help you", and then ask to see the proper approved ID media
- Verify the ID media being worn by the individual is indeed valid for that specific regulated location
    - This is to include SIDA badges, EAA badges, government agency IDs i.e. TSA badge/credentials
- When challenging an individual always compare the photo on their ID media to their face for identity authentication
- Ensure the ID being worn by the individual has not expired

Original Date: 12/10/07



Eliminate

- If the person does not have an ID, notify a UPS management person, who will contact security.
- Unauthorized individuals discovered in a regulated location without ID media must be escorted and immediately reported to a UPS management person who will contact security

Reporting Suspicious Activities

UPS employees and Authorized Representative employees must remain particularly alert to:

- Suspicious or unusual behavior
- Threats against UPS facilities, aircraft, packages, personnel, etc.
- Unusual inquiries about aircraft, cargo, facilities, flight schedules, security measures, etc.
- Surveillance activities by strangers
- Unauthorized attempts to gain access to restricted areas
- Unoccupied vehicles parked conspicuously near regulated locations
- Boxes, bags or other items left unattended near regulated locations (Do not forward or handle a suspicious item)
- Individuals wearing UPS uniforms but are not employees (UPS uniforms or other assets must not be sold or otherwise made available to the public)

These types of suspicious activities could be received in many different forms such as email, phone, social media, text, word of mouth, etc. In the event that threat information is received, you should gather all pertinent information (i.e. date, time, type of threat, information about caller, details of threat). If you receive any information regarding suspicious activities and/or threats immediately report the incident to a UPS management person, your local Security Department and/or appropriate law enforcement authorities.

Insider Threat Awareness

An insider threat arises when one or more individuals with malicious intent have authorized access to aircraft, facilities, equipment, networks, systems or insider knowledge of security measures and

uses their access or knowledge to assist in or to plan acts of violence. Airport employees are the prospective targets of individuals or terrorist groups seeking to gain insider information. Terrorist groups will try to recruit insiders to covertly assist in their terrorist objectives.

Who could be an insider that may possibly pose a threat?

- Current or former employees
- Contractors
- Authorized Representatives
- Any individual with inside access

During our daily routines we develop a level of comfort and familiarity to our surroundings and may be unaware of the insider threat indicators around us. The majority of employees pose no immediate security threat or risk, but we must remember some insiders do have ill intent or are vulnerable to recruitment by terrorist.

What are the potential indicators of an insider threat?

- Divided loyalties
- Ideological or self-identity belief shifts
- Changes in attitude, morale or work ethic
- Adventure or thrill seeking
- Vulnerable to blackmail
- Feelings of anger or revenge
- Greed or financial difficulty
- Security enthusiast but without a need to know interest in specific security measures
- Suspicious foreign contacts or travel
- Accessing regulated locations outside of normal working hours
- Unexplained changes to required routines or required security measures

There have been several instances in the news where potential threats were prevented because airport employees like you saw warning signs and reported the information. If you identify potential insider threats, immediately report the information to a UPS management person, your local Security Department and/or appropriate law enforcement authorities.

Individual Accountability

Employees are prohibited from possessing a weapon or any item that could be used to inflict bodily harm while on UPS property or while conducting company business.

Security regulations not only apply to UPS Airlines and Authorized Representative companies, but also to individual employees responsible for putting their security training into action. Under TSA regulations, individuals trained to perform specific security duties can be held accountable for any event resulting from their non-compliance. Individuals can be fined up to $2,500 for failing to comply with security regulations and for not carrying-out the security procedures which they have been trained to perform. Failing to comply with UPS procedures or TSA regulation can result in disciplinary action up to and including termination.

Notably, the TSA can hold *you* personally responsible and issue *you* a civil penalty.

Following these simple steps will ensure the safe and secure movement of cargo.