Repair Station Training

Repair Station Facility Security

Providing Security Specifically for Repair Stations

Information & References

Basic Safety United States Postal Service
Plan for Mail Safety
http://www.usps.com/

OSHA Right To Know
Hazardous Communication
http://www.osha.gov/

United States Chamber of Commerce
Common Sense Guide for Cyber Security
http://www.us-cert.gov/

Homeland Security
http://www.dhs.gov/dhspublic

National Transportation Safety Board Aviation
http://ntsb.gov/

FAA
Reporting Safety and Security Concerns
http://www.faa.gov/utilities/contactus.cfm

Computer Crime and Intellectual Property Theft
http://www.cybercrime.gov/

The Goal of *Repair Station Security Facility* Training

Facility security must meet certain requirements to provide the level of protection necessary for the business of maintaining articles. The goal of Repair Station Facility Security Training is to present an overview of security issues present in the typical repair station. This will aid the student in understanding the basic elements of security in the repair station environment necessary to provide a safe place to work and maintain articles that meet airworthiness standards.

Outline of *Repair Station Facility Security* Training

I. Introduction
Understanding the Potential Threats

II. The 7 Layers of Security

III. Summary of Goals

IV. Regulatory Requirements

Repair Station Training

Repair Station Facility Security

Providing Security Specifically for Repair Stations

Threat Factors

Threat Assessment

Take a few moments to consider the context of your particular repair station in relationship to potential threats.

___

What environmental factors impact your particular repair station facility?

Consider:
Location (high crime area, isolated, congested, crowded, industrial, airport etc...)

Weather patterns (electrical storms, flooding, excessive cold or heat etc...)

____

What types of maintenance functions do you perform that have a bearing on safety and security?

Consider:
(Classified equipment, contract work for a prime, exotic highly specialized equipment etc...)

Potential Threats for the Typical Repair Station

Repair Station Security is a general subject. The level of security varies from one repair station to another. This training session is designed to evaluate basic security issues that concern every repair station.

I. Introduction **Understanding the Potential Threats**

Potential threat factors includes, theft, disaster, accidents, violence and negligence.

1. Theft is a threat to every business establishment. The typical repair station houses expensive test equipment including computers, electronics, office equipment and parts. Avionics, aircraft engine parts and aircraft accessories are not typical targets of common burglary, but these items are almost always very expensive. Also, the potential for theft of intellectual property, digital theft and parts inventory exists.

2. What happens to business when a disaster hits? The loss of utilities to a facility can severely hamper operations. Tornadoes, earthquakes, electrical storms, and hurricanes represent potential threats to business operations.

3. Accidents occur daily in repair stations across the United States. The potential for accidents in repair stations are high due to the nature of the work. Servicing aviation related items brings workers into contact with high energy electrical equipment, harmful chemicals, heavy weight, shifting loads, and dangerous circumstances.

4. Violence in the work place is on the rise in America. Troubled co-workers, ex-employees, and criminal activity associated with business in general offer the potential for planned or random acts of violence.

5. Employee negligence poses an indirect but real threat to the integrity of the maintenance of aircraft related equipment.

7 Layers of Security

7. Boundaries

6. Access Points

5. Safety

4. Sensitive Areas

3. Critical Areas

2. Restricted Areas

1. Need To Know

II. The 7 Layers of Security

These layers represent levels of security that contribute to the protection of facility assets. The layers of security are progressive - moving from the simplest, and lowest form of security, to the more complex and restrictive.

Layer 7 Security around the perimeter of the facility

The seventh and most general level of security occurs around the perimeter or physical boundary of the facility.

These boarders may include transitional barriers like streets, retaining walls, fences, parking lots, and exterior walls.

The level of security may vary from none to armed security personnel.

The types of security may include fences, gates, surveillance cameras, lighting, guards or a combination of these.

There are many contributing factors for differing levels of security from one facility to another.

For example. A Repair Station that services fuel cells may include an aircraft hangar and ramp as part of their facility. In a case like this airport security may influence the level of security at the Repair Station.

An Avionics Repair Station may be located miles from an airport in a high crime area. This particular Repair Station may use a fence around the perimeter of the facility to protect employee’s vehicles and discourage walk up traffic.

Another Repair Station that services engines and business jet aircraft may work two shifts. This company may want to increase security lighting around the perimeter of the building for safety as well as security reasons.

Layer 7 continued

Locks, alarms, and security patrols are traditional, time tested ways to lock down building during the off hours when the facility is not in use .

The goal of security on the outer boundaries of any repair station facility should address the need for minimizing casual traffic in and around the facility for safety and security reasons.

Layer 6 Security for the entrance and exit points

The sixth layer of repair station facility security includes all ingress and regress points to a building. These facility access points may include, a front entrance, an employee entrance, shipping, receiving, and emergency exits . Other points of access may include windows, the roof, or ceiling when evaluating access points to a facility for safety and security purposes. All possible openings must be considered.

Once again, the strategy employed to restrict access to a facility varies. But it is safe to say that all Repair Stations should utilize some types of security measures to protect their assets.

The front entrance to the facility may be protected by something as simple as a person working at a desk to an electronic keypad entry system. Visitor logs located in the facility's reception area is a simple way to track visitors. Closed circuit cameras may monitor record, and electronically report any visitor who walks through the door. Electronic systems may be tied to cameras, emails, or phones. Any entry into your facility may be monitored, recorded, and reported in real time.

If the perimeter of the Repair Station is not secure then Shipping and Receiving may be more vulnerable to access or theft. Most busy Repair Stations have freight carriers and vendors coming and going throughout the course of a day. Shipping and Receiving may become an informal way for visitors to gain entrance to the facility and avoid the hassle of "signing in" or going through other types of security procedures.

Time clocks may monitor and report when an employee checks in for work. However, they provide no means of monitoring or securing the facility. Often the employee entrance is one of the less restricted access points in a Repair Facility because of the need to accommodate the entrance and exit of several people in a short period of time. Like Shipping and Receiving the Employee Entrance may be used *and abused* by visitors familiar to the facility.

Layer 6 continued

There are several ways to protect these informal entrance points to the Repair Station. Increasing the security around the perimeter of the facility reduces or restricts traffic in these areas. Locks and electronically enabled access points restricts who may utilize these entrances. Obvious surveillance of access points serves as a deterrent to unauthorized access or inappropriate behavior. Posting signs requesting all visitors to use the front entrance may reduce the number of visitors entering through the back entrance. Enforcing policy to keep the loading dock doors down when the access point is not being used for loading or unloading freight will eliminate unauthorized access to this area.

The goal of security at access points is to provide safe and secure access to the repair station facility for employees, visitors, and customers.

Layer 5 Critical Safety Areas

The fifth layer of security involves areas in the facility that pose safety problems.
Many Repair Stations use caustic chemicals, machine shop equipment, test equipment, and various types of tooling.

Some Repair Stations may use fork lifts, hoists, chemical vats, high voltage equipment, and welding equipment. Safety, fire, and hazardous materials training are fundamental training requirements that should be offered to every employee. Aside from this basic training the most effective way to protect employees against injury resulting from the use of equipment, or chemicals is through specialized training. These steps will reduce the occurrence of accidents.

Shop areas devoted to the machine shop, hazardous materials, high voltage equipment, chemical vats and spray booths should be marked. Posting signs with special requirements appropriate to the area serve as a reminder of safe behavior.

For example. When an employee enters the machine shop area they should be reminded to put on safety glasses. When using the paint booth a sign may prompt the employee to turn on the ventilation hood.

Layer 5 continued

For example. An instrument technician is using a 300 Watt, 1000 degree soldering iron to seal an instrument case. During the procedure the shop loses power. The technician feels his way out of the room and exits the building. Because the incident occurred so close to the end of the shift all the employees are released for the remainder of the day. Later that evening the power is restored and the soldering iron begins to heat up. It is resting near a shop towel where it was inadvertently laid when the lights went out. Within minutes the shop towel ignites. An emergency shutdown procedure may have prevented the fire.

The establishment of policy is not adequate. Training will explain the importance of the policy. Reinforcement of the policy and training will underscore the sincerity of management to follow the procedures.

Ramp service areas and aircraft hangars should not be accessible by the general public. Foreign Object Debris, also known as FOD, is a real danger and may be very costly. Often harmful debris migrates into ramp and hangar areas inadvertently. The intake of an engine can ingest harmful debris in a matter of moments. To protect the equipment from exposure to FOD only authorized personnel, who have FOD training should have access to these critical areas. Otherwise someone who has FOD training should accompany visitors.

The goal of the fifth layer of security is to provide a safe work environment for employees. This includes clearly defined safety policy, specialized training, and reinforcement of the safety rules.

Layer 4 Security of Technical Data and Parts

The fourth layer of security involves sensitive areas in the facility. Two areas that may be considered sensitive in any Repair Station are technical data areas and parts inventory. It may not be necessary to restrict access in these areas but access should be monitored and controlled.

FAR Part 145 requires current technical data be made available to technicians servicing articles. To ensure the integrity and availability of technical data it may be necessary to implement a checkout procedure for technical manuals, engineering drawings, and other types of data required for maintenance.

Layer 4 continued

The integrity of parts may be maintained by implementing storage and access procedures. Electrical sensitive parts require special handling and storage procedures. Time dated stock requires procedures to ensure they don't expire. Correct handling and storage of parts will ensure their integrity. Procedures for tracking traceability of parts must be maintained. Documentation must be tracked along with the parts for proper identification. Controlled access to part locations will decrease the risk of unapproved parts entering into your approved parts inventory stream.

At a minimum, access to technical data should include a sign out procedure in a log book. Access to parts may be limited by assigning personnel to manage the supply chain. Inventory security may be determined by the number of employees in the Repair Station.

The goal of the fourth layer of security is to provide availability and integrity of data and parts for the maintenance of articles.

Layer 3 Information and Records Security

The third level of security involves critical areas. These areas may include physical locations as well as access to certain types of information or files.

All company files on computers should be password protected. No unauthorized person should be allowed to alter critical information. Employees may be granted various levels of access to information or programs. Right, or authority to write to files may be granted or denied by assigning levels of access or authorization to each employee.

Critical computer data should be backed up often. There are many different types of backup for computer files. Critical data backups should be stored in a separate location in case of fire, or another type of disaster that takes out original files. Backups may be kept in a fire proof safe or at another secure location. One alternative may be to locate back up files on a secure - remote server.

Layer 3 continued

Hard copy of all data critical to the operations of the Repair Facility should be kept in a location with secure access equal to the online security access. The Repair Station must ensure that their day to day business can continue even if the computer systems were shut down for any reason.

Backup systems protect loss of computer data due to an unexpected abrupt loss of power. An Uninterrupted Power Supply is a battery powered system that allows the user time to recover files in the event of loss of electrical power to the computer. Unlike a backup generator for the entire shop, an uninterrupted power supply is directly connected to the company server, or isolated computer. This power supply is designed to provide a short time of uninterrupted service allowing the user time to properly close out files.

The goal of the third level of security is to provide protection for information and hardware critical for the operation of the company business.

Layer 2 Security in Restricted Areas

The second level of security in a repair station facility involves more restrictive control to areas or information.

Restricted areas in a Repair Station may include Human Resources where personnel information is maintained on computer, or on file.

Sensitive customer information, classified data, or specialized company procedures may require an extra layer of security.

Scrapped parts may require a container or room that is locked to prevent scrapped parts from being recycled back into the supply chain and used in lieu of approved parts.

The Repair Station may store government parts in a Bond Room. This room may require closely guarded access. Initial employee training may include information about these restricted areas. Restricted areas whether they are rooms, closets, or cabinets, should be locked. Employees who have access to these areas should understand company policy concerning who has access to these lock down areas.

Repair Station Facility Security

Providing Security Specifically for Repair Stations

Layer 2 continued

The receiving department and mail room may receive sensitive information on a daily basis. Access to these types of areas may require increased restrictive controls.

Employees working in these areas may require training on identifying suspicious packages. Plan for mail safety. The nation's battle against terrorism takes place on many fronts including the mail rooms of U.S. companies.   A properly informed and well-trained work force can overcome such threats. Employees should be able to quickly identify suspicious packages and letters. Warning signs include.
Misspelled words
No return address
Excessive use of tape
Strange discoloration or odor

The United States Postal Service suggests that if a suspicious letter or package is identified:
Don't open, smell, touch or taste.
Immediately isolate suspicious packages and letters
Move out of the area and don't let others in
Quickly wash with soap and water and remove contaminated clothing.
And finally, contact local law enforcement authorities.

The goal of the second layer of security is to provide a high level of control for the protection of the company, customers and employees.

Layer 1 Security of Classified, Proprietary and Vital Company Information

The final layer of security involves highly restricted or “need to know areas” within the company. These need to know areas include physical locations, and very sensitive information.

Servers typically store information critical to the business of the repair station. The company server should be isolated in a temperature controlled environment, in a room with very limited access. Anyone with access to the server may be able to change pass codes, and alter critical information. The Repair Station’s server should possess password protection, virus protection, and an uninterrupted power supply to avoid problems with the loss or theft of critical data.

Files with Need to Know access may include competitive bids, secret processes, or procedures, that may compromise the operation of the Repair Station if they fell into the wrong hands.

Information critical to the business success or operational success of a Repair Station may be protected by Non-Disclosure Agreements. While a non disclosure agreement does not guard information per se, it does act as a deterrent against the unauthorized disclosure of confidential data.

Repair Stations that service classified equipment or possess classified information may need to include an extra layer of security to exclude the general shop population from access to data hardware and procedures that fall into this category.

The goal of the most restrictive layer of security is to discreetly guard the most vital company information.

III. Summary *Goals of Security*

Layer 7
The goal of security on the outer boundaries of any repair station facility should address the need for minimizing casual traffic in and around the facility for safety and security reasons.

The typical repair station may see many visitors on any given day. Contractors, customers, vendors, and freight carriers have various levels of access to the facility. Steps should be taken to eliminate any unnecessary or unauthorized traffic, this will decrease the potential for incidents within the facility.

Layer 6
The goal of security at access points is to provide safe and secure access to the repair station facility for employees, visitors, and customers.

Steps should be taken to ensure visitors and customers enter the facility at the correct access points. This will decrease the potential of visitors or customers entering areas that are restricted to employees only.

Layer 5
The goal of the fifth layer of security is to provide a safe work environment for employees. This includes clearly defined safety policy, specialized training, and reinforcement of the safety rules.

Safety policy defines expected behavior within the facility. Training demonstrates how policy and procedures are practiced. Reinforcement underscores the necessity of obeying the rules and following the procedures learned in the training process.

Summary Goals of Security continued

Layer 4
The goal of the fourth layer of security is to provide availability and integrity of data and parts for the maintenance of articles.

Regulatory requirements makes the integrity of data and parts key issues for every repair station. Appropriate security measures must be taken to ensure mechanics and technicians have access to current technical approved data to perform service on articles. Training, processes, procedures and security measures must be implemented to ensure only approved parts are used in the maintenance of articles.

Layer 3
The goal of the third level of security is to provide protection for information and hardware critical to the operation of the company business.

Critical information is typically protected by an increased form of security such as restricted access. This type of information may be kept in locked files cabinets or stored on localized computers or the company server. Computers should be password protected and files should be backed up. Information critical to operations must be available even if the company server goes down for any reason. Steps should be taken to ensure the availability of information, records, forms etc...

Layer 2
The goal of the second layer of security is to provide a high level of control for the protection of the company, customers and employees.

In a post 9-11 world we must be proactive in the battle against terrorism. Training for the identification of suspicious packages that arrive at the repair station facility will equip employees who work in these areas.

Summary Goals of Security continued

Layer 1
The goal of the most restrictive layer of security is to discreetly guard the most vital company information.

Most repair stations keep records considered to be confidential. These types of records may consist of employee records, sales agreements, business plans, specialized procedures and processes. To ensure confidentiality access may be restricted to a “need to know” basis.

Some repair stations may have occasion to work on classified equipment. In cases such as this the company may need to restrict access to employees with special clearances.

IV. Regulatory Requirements

145.103 Housing and facilities requirements.

(a) Each certificated repair station must provide—

(1) Housing for the facilities, equipment, materials, and personnel consistent with its ratings.

(2) Facilities for properly performing the maintenance, preventive maintenance, or alterations of articles or the specialized services for which it is rated. Facilities must include the following:

(i) Sufficient work space and areas for the proper segregation and protection of articles during all maintenance, preventive maintenance, or alterations;

(ii) Segregated work areas enabling environmentally hazardous or sensitive operations such as painting, cleaning, welding, avionics work, electronic work, and machining to be done properly and in a manner that does not adversely affect other maintenance or alteration articles or activities;

(iii) Suitable racks, hoists, trays, stands, and other segregation means for the storage and protection of all articles undergoing maintenance, preventive maintenance, or alterations;

(iv) Space sufficient to segregate articles and materials stocked for installation from those articles undergoing maintenance, preventive maintenance, or alterations; and

(v) Ventilation, lighting, and control of temperature, humidity, and other climatic conditions sufficient to ensure personnel perform maintenance, preventive maintenance, or alterations to the standards required by this part.

(b) A certificated repair station with an airframe rating must provide suitable permanent housing to enclose the largest type and model of aircraft listed on its operations specifications.

(c) A certificated repair station may perform maintenance, preventive maintenance, or alterations on articles outside of its housing if it provides suitable facilities that are acceptable to the FAA and meet the requirements of §145.103(a) so that the work can be done in accordance with the requirements of part 43 of this chapter.

Regulatory Requirements *continued*

A Repair Station must provide facilities adequate to meet the regulatory requirements located in Part 145.103

The construction of the facility, environmental features, equipment, utilities, and storage are all given special consideration to ensure they meet the demands of the regulatory requirements.

Sound facility and safety procedures will ensure a safe work environment in which articles will be maintained, stored and protected.