Security of the Mail

Best Practices for Mail Center Security

Incoming and Outgoing Operations

Presented by the United States Postal Inspection Service

There are millions of businesses that use the mail. The vast majority of these have only 'one to a few' person(s) responsible for mail center-type operations. Of these millions of businesses, there are thousands of large, complex corporate mail center operations. The best practices listed below are a summary of well-developed mail center security procedures that can be used by any mail center. **Procedures applicable primarily to large mail centers are identified as such, and *in bold*.**

These recommendations come from businesses that use the mail and have been shared with the USPS for distribution to its customers. Since needs and resources are often different, every suggestion may not apply to all businesses. Mailers should determine which are appropriate for their company and conduct periodic security reviews of their operation to identify needed improvements. The list below contains general security concepts and a few specific examples of how to accomplish them.

General Mail Operation preventive recommendation:

- Appoint a Mail Security Coordinator (and an alternate if a large mail center)
- Organize a Mail Security Response Team, as practical, depending on the size of the mail center staff
- Create, update and/or review SOPs, Security Procedures, Disaster Plans, and Operating Plans. **Keep a back-up copy of plan(s) off-site.**
- Train personnel in policies and procedures relative to mail security, i.e. biological, chemical, weapons or natural disasters
- Include from the staff, when possible, certified firefighters, biohazard handlers, and/or corporate safety, environment and health personnel, or, train personnel in these duties
- Members of the team should be equipped with cell phones/pagers and should be available up to 24 hours a day, 7 days a week, as is appropriate for the situation
- Information, and updates, about the personnel and response procedures should be published and distributed company-wide
- Federal Government Mail Managers should also refer to the General Services Administration (GSA) web site for specific and updated information concerning federal mail management policies and procedures
- Publish an After-Action Report or Incident Report after every incident
- Have senior management buy-in/sign-off on company's mail security procedures

Employee Security Procedures

- Maintain good hiring practices
  - Provide in-depth screening/background checks when hiring new employees

- Make arrangements with one or two temporary employment agencies to ensure that a restricted, pre-screened group of individuals is available when needed to supplement the workforce
- Enforce/institute probationary period for evaluation of employees

- Establish a strict employee identification/personnel security program
  - Require employees to wear photo ID badges at all times
  - Instruct employees to challenge any unknown person in a facility
  - Where provided to employees, utilize uniforms with names and logos stitched on them for employees to wear at work
  - Provide a separate and secure area for personal items (e.g., coats and purses). Prohibit employees from taking personal items into the main workspace
  - Establish incoming/outgoing personal mail procedures
  - **Hire or designate security personnel for mail center area. (Primarily for large mail centers.)**
- Establish health safety procedures
  - **Have on-site medical personnel (large mail center) or arrange for off-site facility/personnel**
  - Encourage employees to wash hands regularly, especially prior to eating
  - Encourage employees to see doctor if suspicious symptoms occur
  - Encourage employee attendance in health seminars, talks, info updates
  - As practical, establish or take advantage of company health programs, i.e. shots, check-ups
  - Provide approved personal protection equipment according to CDC guidelines

General Safety and Security Procedures for Incoming/Outgoing Mail Areas

- Notify internal and external customers, as appropriate, of steps taken to ensure safety of mail
- Control or limit access of employees, known visitors and escorted visitors to the mail center with sign-in sheets, badges, and/or card readers. **(For large mail operations, include plant, workroom floor, etc.)**
- Subject to emergency exit safety requirements, lock all outside doors and/or prohibit doors from being propped open
- Require deliveries to be made in a restricted, defined area
- Restrict drivers (rest areas) to an area that is separate from the production/mail center facilities.
- Use video cameras inside and outside the facility/docks, as feasible
- Keep the area for processing incoming and outgoing mail separate from all other operations, as feasible
- If a separate processing area is used, it should not be part of the central ventilation system
- Shut-off points of processing area's ventilation system should be mapped and should be part of an emergency procedures handout
- Separate processing area should include appropriate personnel protection equipment and disposal instructions for such equipment, as approved by the CDC
- Designate and publish/post evacuation routes for emergency situations
- Conduct training, emergency preparedness drills, and information update meetings, as necessary
- **X-ray all incoming mail. (Large mail centers.)**
- Maintain a Suspicious Package Profile
- Ensure appropriate emergency access numbers are posted by or on every phone. Such numbers should include: call 911; CDC at 770-488-7100; local Postal Inspector; or local police or fire department
- Maintain updated employee lists (name, address, phone/cell phone), and keep back-up copy off-site
- Provide only vacuum systems for cleaning equipment, not forced air systems
- If not already done, alter receiving procedures to require a manifest with all shipments and practice the acceptance of "complete" shipments only
- Discarded envelopes, packages, boxes should be placed in a covered container and transported to the loading dock for removal. (Ensure local arrangements are in place for disposal of such material.)

Access to Information - Education and Communications

- Maintain a library of publications, videos, brochures, from appropriate information sources, and facilitate employee access to them as needed. Sources should include USPS, CDC, and OSHA
- Maintain and publish a list of useful websites from appropriate authoritative sources. Bookmark appropriate web sites for easy access, i.e. CDC, OSHA, USPS, and GSA. Monitoring twice a day is a minimum recommendation, as situations warrant
- Maintain and publish list of phone numbers to call in an emergency - Postal Inspectors, Fire Dept., CDC, OSHA, Police, etc.
- Present updated Best Practices from CDC, OSHA, GSA, USPS, and Fire Dept.
- Company-wide communications concerning mail center security procedures should be implemented
- Require/encourage applicable employees to attend all local meetings pertaining to mail security issues

Guidelines for Mail Center Theft Prevention

Mail is sometimes lost or stolen from company mail centers, or while en route to or from the Post Office. Much of this mail is quite valuable, containing cash, jewelry, and other high-value items. Needless to say, such losses are costly to the company and its investors. The following are some suggestions for improving theft prevention in your mail center operation:

- Know your employees. Don't put your new hires in your mail center without a criminal record check.
- Secure your mail center. Prevent access by unauthorized persons. Keep locked whenever possible, especially when no one is on duty. Maintain a sign-in sheet for persons entering and leaving the mail center, including times of arrival and departure.
- Registered Mail™. Keep separate from other mail. Document transfer of Registered Mail by requiring the receiver to sign for custody.
- Protect company funds. If company funds are handled as part of the mail center operations, establish adequate controls to fix individual responsibility for any losses that may occur.
- Keep postage meters secure. Postage meters should be secured when not in use. Check mails periodically to determine if employees are using company postage meters for their personal mail.
- Vary times and lines of travel between post office and plant. If currency or other valuable mail is sent or received, check periodically to see if mail messengers are making unauthorized stops or is leaving mail unattended in unlocked vehicles.
- Employees caught stealing should be prosecuted. There is no greater deterrent to a potential thief than the fear that he/she may go to jail. The Postal Inspection Service will extend its full cooperation.

Some Critical Websites - bookmark for quick reference: (include your various suppliers/vendors)

US Postal Service - www.usps.com
Centers for Disease Control (CDC) - www.cdc.gov
Occupational Safety and Health Administration (OSHA) - www.osha.gov
General Services Administration (GSA) - www.gsa.gov
Federal Bureau of Investigation (FBI) - www.fbi.gov
Bureau of Alcohol, Tobacco and Firearms (BATF) - www.atf.treas.gov