Food Defense Best Practices

The following are food defense best practices that should be integrated into the everyday practices of a retail food establishment. These are adapted from the *Guidance for Industry: Food Security Preventive Measures Guidance for Retail Food Stores and Food Service Establishments,* which can be accessed on the FDA website.

GENERAL

Prepare for the possibility of tampering or other malicious, criminal, or terrorist actions.

- Assign responsibility for security to knowledgeable individual(s)
- Conduct an initial assessment of food security procedures and operations, which we recommend be kept confidential
- Have a crisis management strategy to prepare for and respond to tampering and other malicious, criminal, or terrorist actions, both threats and actual events, including identifying, segregating and securing affected product
- Plan for emergency evacuation, including preventing security breaches during evacuation
- Become familiar with the emergency response system in the community
- Make management aware of 24-hour contact information for local, state, and federal police/fire/rescue/health/homeland security agencies
- Make staff aware of whom in management they should alert about potential security problems (24-hour contacts)
- Promote food security awareness to encourage all staff to be alert to any signs of tampering or other malicious, criminal, or terrorist actions or areas that may be vulnerable to such actions, and reporting any findings to identified management (for example, providing training, instituting a system of rewards, building security into job performance standards)
- Have an internal communication system to inform and update staff about relevant security issues
- Have a strategy for communicating with the public (for example, identifying a media spokesperson, preparing generic press statements and background information, and coordinating press statements with appropriate authorities)

Supervision

- Provide an appropriate level of supervision to all staff, including cleaning and maintenance staff, contract workers, data entry and computer support staff, and especially, new staff (for example, supervisor on duty, periodic unannounced visits by supervisor, daily visits by supervisor, two staff on duty at same time, monitored video cameras, off-line review of video tapes, one-way and two-way windows, customer feedback to supervisor of unusual or suspicious behavior by staff)
- Conduct routine security checks of the premises, including utilities and critical computer data systems (at a frequency appropriate to the operation) for signs of tampering or malicious, criminal, or terrorist actions or areas that may be vulnerable to such actions

Free food defense training available

- Food Defense 101 Training for Frontline Employees: https://www.fda.gov/food/food-defense-tools-educational-materials/food-defense-101-front-line-employee

- Employees First Training: https://www.fda.gov/food/food-defense-tools-educational-materials/employees-first

FACILITY

Restricted Access

- Identify staff that require unlimited access to all areas of the facility
- Reassess levels of access for all staff periodically
- Limit staff access to non-public areas so staff enter only those areas necessary for their job functions and only during appropriate work hours (
- Change combinations, rekey locks and/or collect the retired key card when a staff member who is in possession of these is no longer associated with the establishment, and additionally as needed to maintain security

Physical Security

- Use metal or metal-clad exterior doors to the extent possible when the facility is not in operation, except where visibility from public thoroughfares is an intended deterrent
- Minimize the number of entrances to non-public areas
- Account for all keys to establishment (for example, assigning responsibility for issuing, tracking, and retrieving keys)
- Monitor the security of the premises using appropriate methods (for example, using security patrols [uniformed and/or plain-clothed], monitored video surveillance)
- Minimize places in public areas that an intruder could remain unseen after work hours and places in non-public areas that can be used to temporarily hide intentional contaminants (for example, minimizing nooks and crannies, false ceilings)
- Provide adequate interior and exterior lighting, including emergency lighting, where appropriate, to facilitate detection of suspicious or unusual activities

Storage and Use of Poisonous and Toxic Chemicals in non-public areas

- Store poisonous and toxic chemicals as far away from food handling and storage areas as practical
- Limit access to and securing storage areas for poisonous or toxic chemicals that are not being held for retail sale (for example, using keyed or cipher locks, key cards, seals, alarms, intrusion detection sensors, guards, monitored video surveillance [remember to consult any relevant federal, state, or local fire codes before making any changes])
- Ensure that poisonous and toxic chemicals are properly labeled
- Use pesticides in accordance with the Federal Insecticide, Fungicide, and Rodenticide Act (for example, maintaining rodent bait that is in use in covered, tamper-resistant bait stations)
- Know what poisonous and toxic chemicals should be on the premises and keeping track of them
- Investigate missing stock or other irregularities outside a normal range of variation and alerting appropriate law enforcement and public health authorities about unresolved problems, when appropriate

EMPLOYEES

Screening

- Examine the background of all staff (including seasonal, temporary, contract, and volunteer staff, whether hired directly or through a recruitment firm) as appropriate to their position, considering candidates' access to sensitive areas of the facility and the degree to which they will be supervised and other relevant factors (for example, obtaining and verifying work references, addresses, and phone numbers, and/or having a criminal background check performed by local law enforcement or by a contract service provider

Identification

- Establish a system of positive identification and recognition that is appropriate to the nature of the workforce (for example, issuing uniforms, name tags, or photo identification badges with individual control numbers, color coded by area of authorized access), when appropriate
- Collect the uniforms, name tag, or identification badge when a staff member is no longer associated with the establishment

Personal Items

- Restrict the type of personal items allowed in non-public areas of the establishment
- Allow in the establishment only those personal use medicines that are necessary for the health of staff and ensuring that these personal use medicines are properly labeled and stored away from stored food and food preparation areas
- Prevent staff from bringing personal items (for example, lunch containers, purses) into nonpublic food preparation or storage areas
- Provide for regular inspection of contents of staff lockers (for example, providing metal mesh lockers, company issued locks), bags, packages, and vehicles when on company property (Remember to first consult any federal, state, or local laws that may relate to such inspections)

Training in Food Security Procedures

- Incorporate food security awareness, including information on how to prevent, detect, and respond to tampering or other malicious, criminal, or terrorist actions or threats, into training programs for staff, including seasonal, temporary, contract, and volunteer staff
- Provide periodic reminders of the importance of security procedures (for example, scheduling meetings, providing brochures or payroll stuffers)
- Encourage staff support (for example, involving staff in food security planning and the food security awareness program, demonstrating the importance of security procedures to the staff)

Visitors (for example, contractors, sales representatives, delivery drivers, couriers, pest control representatives, third-party auditors, regulators, reporters, tours)

- Restrict entry to the non-public areas of the establishment (for example, checking visitors in and out before entering the non-public areas, requiring proof of identity, issuing visitors badges that are collected upon departure, accompanying visitors)
- Ensure that there is a valid reason for all visits to the non-public areas of the establishment before providing access to the facility - beware of unsolicited visitors
- Verify the identity of unknown visitors to the non-public areas of the establishment
- Inspect incoming and outgoing packages and briefcases in the non-public areas of the establishment for suspicious, inappropriate or unusual items, to the extent practical

Deliveries

- Inform suppliers, distributors, and transporters about FDA's food security guidance, "Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance" and "Importers and Filers: Food Security Preventive Measures Guidance," available at: http://www.cfsan.fda.gov/~dms/guidance.html.
- Take steps to ensure that delivery vehicles are appropriately secured
- Request that transporters have the capability to verify the location of the load at any time, when practical
- Establish delivery schedules, not accepting unexplained, unscheduled deliveries or drivers, and investigating delayed or missed shipments
- Supervise off-loading of incoming materials, including off hour deliveries
- Investigate shipping documents with suspicious alterations
- Inspect incoming products and product returns for signs of tampering, contamination, or damage (for example, abnormal powders, liquids, stains, or odors, evidence of resealing, compromised tamper-evident packaging) or "counterfeiting" (for example, inappropriate or mismatched product identity, labeling, product lot coding or specifications, absence of tamper-evident packaging when the label contains a tamper-evident notice), when appropriate
- Reject suspect food
- Alert appropriate law enforcement and public health authorities about evidence of tampering, "counterfeiting," or other malicious, criminal, or terrorist action

Customers

- Prevent access to food preparation and storage and dishwashing areas in the non-public areas of the establishment, including loading docks
- Monitor public areas, including entrances to public restrooms (for example, using security guards, monitored video cameras, one-way and two-way windows, placement of employee workstations for optimum visibility) for unusual or suspicious activity (for example, a customer returning a product to the shelf that he/she brought into the store, spending an unusual amount of time in one area of the store)
- Monitor the serving or display of foods in self-service areas (for example, salad bars, condiments, open bulk containers, produce display areas, doughnut/bagel cases)

Food Service and Retail Display

- Periodically check products displayed for retail sale for evidence of tampering or other malicious, criminal, or terrorist action (for example, checking for off-condition appearance [for example, stained, leaking, damaged packages, missing or mismatched labels], proper stock rotation, evidence of resealing, condition of tamper-evident packaging, where applicable, presence of empty food packaging or other debris on the shelving)
- Monitor self-service areas (for example, salad bars, condiments, open bulk containers, produce display areas, doughnut/bagel cases) for evidence of tampering or other malicious, criminal, or terrorist action