



## **FOOD SECURITY PREVENTIVE MEASURES GUIDANCE FOR FOOD ESTABLISHMENT OPERATIONS**

Food Security-protecting food against deliberate contamination- has become a very real concern for public health and law enforcement officials. The rise of terrorist activity in the U.S. and the availability of information over the Internet on how dangerous agents can be spread by air; water or food fuels this concern. As plans are developed to respond to outbreaks of food borne illness, thought must be given to how to cope with the threats of terrorism. This guide was modified and adapted by the Retail Food Security Committee of the North Carolina's Department of Environment and Natural Resources. These are appropriate measures that can be taken by food service operations to minimize the risk of food being subjected by tampering or terrorist actions.

This guidance is designed as an aid to operators of food service and retail food establishments. It identifies preventive measures that can be taken to minimize the risk to food under their control. Operators of food are encouraged to review their current procedures and controls of the potential for tampering, criminal or terrorist actions and make appropriate improvements. This guidance is designed to focus operators sequentially on each segment of the farm-to fork system that is within their control, to minimize their risks. Implementing enhanced preventive measures requires the commitment of management and employees to be successful and therefore, both should participate in their development and review.

This guidance is divided into seven sections that relate to individual components of a food operation: management of food security; physical security; employees; computer systems; raw materials and packaging; operations; and finished products. It also covers security strategies and evaluation of the security system. Not all of the guidance contained in this document is appropriate or practical for every retail food establishment. Operators should review the guidance in each section that relates to a component of their operation, and assess and implement preventive measures that are suitable for their operation.

### **I. Establishment Operations and Practices:**

#### **Management of Food Security**

Operators of establishments should consider:

##### Security procedures

- assigning responsibility for security to qualified individual(s)
- encouraging all staff to be alert to signs of tampering with product or equipment or systems, or other unusual situations, or areas that may be vulnerable to tampering and to notify identified management about any findings (e.g., provide training, institute a system of rewards, build into job performance standards)

##### Investigation of suspicious activity

- immediately investigating all information about suspicious activity
- alerting local law enforcement about all suspected criminal activity

##### Supervision

- providing an appropriate level of supervision to all employees, including data entry personnel, computer support, cleaning and maintenance staff, and contract workers, and especially new employees
- conducting daily security checks of the premises for signs of tampering with product or equipment, other unusual situations, or areas that may be vulnerable to tampering

##### Mail/packages

- implementing procedures to ensure the security of incoming mail and packages (e.g., secure mailroom, visual or x-ray mail package screening)

#### **Employees**

Operators of establishments should consider:

Pre-hiring screening

- obtaining and verifying work references, addresses, and phone numbers
- performing criminal background checks, including FBI Watchlist [remember to consult any state and local laws that may apply to the performance of such checks]
- checking immigration status with the Immigration and Naturalization Service, if appropriate
- applying these screening procedures to all employees, including seasonal, temporary, contract and volunteer employees

Daily work assignments

- knowing who is and who should be on premises, and appropriate location
- being specific to shift and authority
- keeping assignment information updated

Identification

- establishing a system of positive identification and recognition (e.g., photo identification badges, with individual control numbers, color coded by area of authorized access)
- collecting the retired identification badge when an employee is terminated, either voluntarily or involuntarily

Restricted access

- limiting access to those areas and portions of the operation necessary for the employee's position, including access to data operating systems for purchasing, storing and distributing imported foods (e.g., key card or cypher locks to sensitive areas, color-coded uniforms) [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes]
- changing combinations and/or collecting the retired key card when an employee is terminated and additionally as needed to maintain security
- reassessing levels of access for all employees periodically

Personal items

- restricting personal items allowed in establishment
- preventing employees from bringing personal items (e.g., lunch containers, purses) into food handling areas
- establish a policy and providing for inspection of contents of employee lockers (metal mesh lockers, company-provided locks), bags, and vehicles when on company property

Training in security procedures

- ensuring employee buy-in (e.g., demonstrate the importance of security procedures to the employees themselves)
- providing food security training to all new employees, including information on how to prevent, detect, and respond to tampering or criminal or terrorist activity
- providing periodic reminders of the importance of security procedures

Unusual behavior

- Watching for unusual behavior by new employees or workers (e.g., workers who stay unusually late after the end of their shift, arrive unusually early, access files/information/areas of the facility outside of the areas of their responsibility, remove documents from the facility, ask questions on sensitive subjects, bring cameras to work)

## **Data Systems**

Operators of establishments should consider:

- restricting access to computer operational systems and other critical systems to those with appropriate clearance (e.g., passwords, firewalls)
- eliminating system access immediately upon employee termination
- establishing a system of traceability of computer transactions
- reviewing adequacy of procedures for backing up critical computer-based data systems
- auditing the system routinely to assure security procedures are in place
- validating and periodically challenging the data security system and procedures

## **Physical Security**

Operators of establishments should consider:

Visitors

- inspecting incoming and outgoing vehicles for inappropriate or unusual items or activity
- restricting entry to the establishment (checking in and out at security or reception, proof of identity, visitor badges - collect upon departure)

- ensuring there is a valid reason for the visit before providing access to the facility - beware of unsolicited visitors
- restricting access to food handling and storage areas (accompanied by employee unless specifically authorized)
- restricting access to locker rooms
- applying the above procedures to everyone, including contractors, supplier representatives, truck drivers, customers, couriers, third-party auditors, regulators, reporters, visitors, etc.

#### Physical facility

- protecting perimeter access with fencing or other appropriate deterrent
- securing doors (including freight loading doors), windows, roof openings/hatches, vent openings, trailer bodies, railcars, and storage areas (e.g., locks, seals, sensors, alarms, guards, video surveillance) [remember to consult any relevant state and local fire codes before making any changes]
- using metal or metal-clad doors, to the extent possible, especially when the facility is not in operation
- minimizing the number of entrances to restricted areas [remember to consult any relevant state and local fire codes before making any changes]
- accounting for all keys to the establishment
- using security patrols (uniform and/or plain-clothed) and/or video surveillance, where appropriate
- minimizing places that may serve as temporary hiding places for intentional contaminants (e.g., minimize nooks and crannies)
- providing adequate interior and exterior lighting, including emergency lighting
- implementing a system of controlling vehicles authorized to park on the premises (e.g., placard, decal, key card, cypher lock)

#### Storage of hazardous chemicals (cleaning and sanitizing agents, pesticides)

- securing storage areas for hazardous chemicals (e.g., locks, seals, alarms, sensors) (remember to consult any relevant state and local fire codes before making any changes)
- limiting access to storage areas (use key cards or cypher locks) (remember to consult any relevant state and local fire codes before making any changes)
- inspecting chemicals upon receipt and verifying authenticity
- keeping track of hazardous chemicals
- investigate missing stock or other irregularities outside normal variation and alerting local law enforcement of any unresolved problems

### **Products and Shipments**

Operators of establishments should consider:

#### Suppliers

- using only known, appropriately licensed or permitted (where applicable) sources for all products
- taking steps to ensure that suppliers and transporters practice appropriate food security measures (e.g., auditing for compliance with food security measures that are contained in purchase and shipping contracts or letters of credit)
- authenticating labeling and packaging configuration in advance of receipt of shipment (labeling should be traceable to a specific foreign manufacturing/processing facility)
- inspecting incoming products for authenticity, packaging/product integrity, and evidence of unauthorized relabeling/repackaging (e.g., shipping cases and described contents not consistent with actual contents) and verifying batch/lot/container codes and alerting appropriate authorities of any evidence of tampering, counterfeiting, or sabotage
- verifying conformance with FDA requirements for product safety, quality, effectiveness, and labeling (may require contact with and verification from the foreign manufacturer/processor)
- developing and implementing procedures for inspecting shipping containers, vehicles
- developing and implementing procedures for assessing safety of abnormal powders, odors, liquids present on shipments
- investigating damage and loss and alerting appropriate authority of discrepancies
- requiring transportation companies to conduct background checks of drivers and other employees with access to product (state and local laws may apply)
- requesting locked and sealed vehicles/containers/railcars, obtaining the seal number from the supplier, and verifying upon receipt - make arrangements to maintain the chain of custody when a seal is broken for inspection by a governmental agency
- reconciling the amount received with the amount ordered and the amount listed on the invoice and shipping documents

- reconciling the amount received with any reports of sampling prior to receipt of shipment
- supervising off-loading of incoming products and product returns

#### Security of products

- keeping track of products, including salvage, reworked and returned products
- establishing receiving (examination), quarantine, and release procedures
- investigating missing stock or other irregularities and alerting local law enforcement of any unresolved problems
- ensuring that public storage warehousing and shipping (vehicles and vessels) practice appropriate security measures (e.g., auditing for compliance with food security measures that are contained in contracts or letters of guarantee)
- performing random inspection of storage facilities, vehicles, and vessels for evidence of appropriate and effective security program
- requiring transportation companies and warehouses to conduct background checks on staff (drivers/warehouse personnel) (state and local laws may apply)
- requesting locked and sealed vehicles/containers/railcars and providing the seal number to the consignee (remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes)
- restricting access to distribution process to employees with appropriate clearance
- advising sales staff to be on the lookout for counterfeit products during visits to customers and notify management of any problems
- alerting local law enforcement about evidence of tampering or counterfeiting

## **II. Security Strategy:**

Operators of establishments should consider:

### **Response to tampering or criminal or terrorist event**

- having a step-by-step strategy for triaging the event
- planning for emergency evacuation, including preventing security breaches during evacuation
- having investigation procedures
- identifying critical decision-makers
- identifying management to whom employees should report potential security problems
- identifying local, state, and federal police/fire/rescue/government contacts
- identifying a media spokesperson
- having a generic press statements and background information

### **Recall strategy**

- identifying the person responsible, and a back-up
- providing for proper disposition of recalled product
- identifying customer contacts, addresses and phone numbers

### **Additional steps**

- maintaining any floor or flow plan in secure, off-site location
- having internal, fire, and police emergency phone numbers available to appropriate employees
- making employees aware of the company officials to alert about potential security problems, and where they can be reached
- becoming familiar with the emergency response system and the Emergency Command Center operations in the state in which the facility is located

### **Data Systems**

- having contingency plans
- having a back-up database and electronic inventory
- restricting emergency access to employees with appropriate clearance

### **III. Evaluation Program:**

Operators of establishments should consider:

- evaluating the lessons learned from past tampering or security threats
- annually reviewing and testing the effectiveness of strategies (e.g., conducting mock criminal, terrorist or tampering event and mock recall, challenging computer security system) and revising accordingly - using third party or in-house security expert
- performing routine, random, and documented food security inspection of facility (using third party or in-house security expert)
- verifying that security contractors are doing an adequate job

#### **Emergency Point of Contact:**

## **Local Law Enforcement 911**

#### **Vulnerability Assessment and Security Coordination:**

#### **Local Law Enforcement**

#### **Other interested points of contact:**

#### **Local Public Health Department**

The Retail Food Security committee that developed the Guidance document is composed of the following members :

- Steve Tracey, Food Lion, North Carolina Food Dealers Association
- Ted Rhodes, North Carolina Restaurant Association
- Dave Grouewoller, North Carolina Restaurant Association
- Stacy Covil, K & W Cafeteria, Retail Food Industry
- Don Womble, Hoke County Health Department, Local Health Directors
- Tony Noonan, Pope and Sons, North Carolina Convenience Store Association
- Pamela Jenkins, Communicable Disease Branch NP, Interagency Food Security
- Mary Reese, Cherry Hospital Dietician, North Carolina Dietary Association
- Will Service, North Carolina Department of Health and Human Services, NC BT team
- Terry Bolick, Catawba County Health Department, Western Educational District of NCPHA
- Lynn Van Dyke, Craven County Health Department, Eastern Educational District of NCPHA
- Sue Grayson, North Carolina Department of Environment, and Natural Resources, Dairy and Food Protection
- Melissa Renfrow, North Carolina Department of Environment, and Natural Resources, Regional Environmental Health

