Practical Guidance
Food Defense and Agricultural Security Community

PHYSICAL SECURITY GUIDANCE

FOR THE FOOD AND BEVERAGE

INDUSTRY TO ENHANCE FOOD DEFENSE OUTCOMES

INSTALLMENT #1 – NOVEMBER 2021

The ASIS Food Defense and Agriculture Security Steering Committee created this resource for the global food and beverage manufacturing community.
Originally published: November 2021

Founded in 1955, ASIS International is a global community of security professionals, educators, and practitioners, all of whom has a role in the protection of assets - people, property, and/or information.

Our members represent virtually every industry in the public and private sectors, and organizations of all sizes. From entry-level managers to Chief Security Officers (CSOs) to CEOs, from security veterans to consultants and those transitioning from law enforcement or the military, the ASIS community is global and diverse.

The following members of the ASIS Community tirelessly volunteered their time to produce this guidance document for the global food and beverage manufacturing committee:

Name	Company	Contact Information
Rich Widup	Reckitt	richard.widupjr@mjn.com
Jason Bashura	PepsiCo	jason.bashura@pepsico.com
Frank Pisciotta	Business Protection Specialists	fp@securingpeople.com
Alan Waggoner	Siemer Milling Company	awaggoner@siemermilling.com
Matt Sholly	Clemens Food Group	msholly@clemensfoodgroup.com
Todd Pooler	Danone North America	todd.pooler@danone.com
Rod Pearson	Impossible Foods Inc.	roderick.pearson@impossiblefoods.com

Table of Contents

The ASIS Food Defense and Agriculture Security Steering Committee created this resource for the global food and beverage manufacturing community.
Originally published: November 2021

The ASIS Food Defense and Agriculture Security Steering Committee created this resource for the global food and beverage manufacturing community.
Originally published: November 2021

Scope and Introduction

Food and Beverage Threats

There are several threats to the food and beverage industry and while the threats may originate from external sources, there is a far greater likelihood that threats will originate from insiders. A model which was developed to address workplace violence offenders can also be applied to the food and beverage industry to illuminate the most likely insider sources.

Type	Description	Potential Motivation
1	Criminal Intent, Outsider	Behavioral Health Patient Social Media Fame Seeker Copycat Extortion Economic motivation
2	Truck Driver	My load isn't ready, you are costing me money
3	Current/Former Employee or Contractor	I am upset with a coworker and adulterate to create problems for that person * I am upset with the company and adulterate as retribution and to harm the brand * Youthful stupidity I am not paid enough *
4	Domestic or intimate partner driven	I am upset with a coworker and adulterate to create problems for that person
5	Ideological	Radicalized Insider, terroristic intent, wide scale public health impact

* - Supported by actual incidents

Internal threat sources represent the greatest potential risk to food and beverage enterprise; therefore this document has organized to address the most sensitive internal areas and work outwards toward the perimeter; whether that be the building or perimeter fence.

External Threat Sources include individuals who have no direct relationship with the business who may be motivated by terrorists (human and cyber), extremists with radical ideologies, or "value-driven" groups who feel justified by their beliefs.

Identifying Risk

Food defense is the effort to protect food and beverage products from acts of contamination and adulteration where there is an intent to cause harm to consumers, or as an act of revenge or in response to a grievance against an individual or the company. In the United States, the Food Safety Modernization Action (FSMA) Final Rule for Mitigation Strategies to Protect Food Against Intentional Adulteration, establishes a framework for regulated facilities which largely covers the Type 5 ideological offender which attempts to solve for some of the risk in the form of "wide-scale public health impact". This document is intended to serve an international audience, organizations of all sizes and provide guidance for protecting food and beverage operations from all insider threats.

The ASIS Food Defense and Agriculture Security Steering Committee created this resource for the global food and beverage manufacturing community.
Originally published: November 2021

Regardless of where the facility is located, it is in the best interests of food and beverage facilities (hereafter facilities) to identify and reduce the risk of acts of intentional adulteration (hereafter contamination). Facilities should closely evaluate and assess internal and external threat sources and resulting risk accordingly.

This document is not intended to teach organizations how to conduct a detailed risk assessment for facilities, but rather provide clarity on the difference between a vulnerability and a risk assessment. The common elements of a food defense risk assessment a team may follow are described below:

Step	Description
1. Asset Characterization	Asset characterization includes analyzing information that describes technical details of production processes required to support analysis, identifying critical assets, identifying hazards and consequences of contamination, and identifying existing layers of protection.
2. Threat Assessment	Consideration of human hazards should include internal threats, external threats, and internally assisted threats (e.g., collusion between insiders and outsiders). The selection of the threats should include historical incident history in the food and beverage industry, reasonable local, regional, or national intelligence information, where available.
3. Vulnerability Identification	Determining where product may be susceptible to contamination.
4. Risk Analysis	The risk assessment determines the relative degree of risk to the facility in terms of the expected effect of various product contamination scenarios as a function of consequence and probability of occurrence.
5. Mitigation Identification and Food Defense Master Planning	The team will brainstorm options for reducing the vulnerability to high risk contamination scenarios identified in the process. Mitigation strategies should be prioritized and presented to facility leadership for consideration and implementation.
6. Update the Food Defense Plan	As additional mitigation strategies are implemented, the food defense plan should be updated and additional training provided as appropriate.
7. Reanalysis and Reassessment	Risk should be reassessed periodically, at leadership request, as a result of an incident or when any significant changes are made to the facility or process.

As the risk assessment is being conducted this document can be used to consider strategies that will decrease the likelihood that an adversary can successfully contaminate a product, increase deterrence and more quickly detect violations of food defense measures.

Document Assumptions and Limitations

- This document is intended to reduce the risk of product contamination. Its scope is limited to production processes and ends when the product is in tamper evident packaging.
- Food defense in the context of this document extends beyond wide scale public health impact and the radicalized insider.

Identification and Protection of Vulnerable Areas

Labs

From a product contamination perspective, a lab may contain reagents and other materials (that could be used as a contaminant) that are legitimately needed to support operations. Such materials must be protected from unauthorized access by a person intending on contaminating food or beverage production. Further, sound inventory control programs are another "layer" of protection assuring that these materials cannot be used for an act of contamination.

Physical security and access control measures for labs should be considered and implemented based on site-specific risk assessment. This may vary by site and depends on the lab's location in the facility. Common security measures might include electronic access control to manage entry, lock and key control, cameras, door alarms, door logs, additional supervision, container security (e.g., locked and potentially alarmed chemical storage), color-coded uniforms or bump caps to designate work area, and limiting personal items in the lab.

Fail-secure electronic locksets may be specified in lab situations to prevent unauthorized access to the facility if primary and backup power is lost. A fail-secure system requires power to unlock the door thus preventing circumventing of the security system by cutting power. Fail-secure locksets typically include key override to allow access by appropriate personnel in power outages. A door position switch can monitor door position for a variety of purposes and notify security personnel if it detects a door has been physically forced open or held open beyond the permissible time set in the software (e.g., 30 seconds).

Security cameras are desirable in lab settings. These observation cameras can be an important safety and security feature especially in high-security labs where windows are undesirable. Many different camera types may be employed depending on the function. Security cameras typically are installed with a fixed field of view pointing directly at the item or area that is being monitored, (e.g., a lab entrance, freezer with sensitive samples).

Additional lab security measures should include maintaining a strict inventory and training. Appropriate personnel should always know where and how much hazardous materials are stored in the lab. Unaccounted loss of these materials should be reported immediately to security personnel and thoroughly investigated to determine the root cause and to determine if product has been impacted. Lab personnel should be appropriately trained on lab security procedures and why they are important.

Finally, lab personnel should have basic or general food defense awareness training that can support and drive future success of the site's food defense program.

Mixing and Weighing Areas

Mixing and weighing rooms are potentially vulnerable areas where a substance could be introduced to contaminate food products. The substance could be evenly mixed within the product and affect all the servings producing a contaminated batch. Attacks in these settings would likely be an insider. Therefore, it is critical facilities implement effective mitigation strategies to reduce the vulnerabilities that might be present in these areas.

Facilities should conduct site-specific risk assessment to learn of vulnerabilities unique to the site. Risk assessments should be periodically revisited and modified as necessary; typically, on a 3–5-year recurring cycle, or when on site conditions, staff load, or other factors within the facility change that could impact the outcomes of the previously completed risk assessment.

In 2011, the FDA released the Food Defense Mitigation Strategies Database available for public use at https://www.cfsanappsexternal.fda.gov/scripts/fooddefensemitigationstrategies/index.cfm. The Food Defense Mitigation Strategies Database (hereafter FDA Database) contains an extensive listing of mitigation measures that may be useful in reducing contamination vulnerabilities that might exist in the facility's operations. The FDA Database can be browsed by categories (e.g., conveyance, material handling, packaging, processing, key activity types, storage, transportation/distribution). Another way to classify mitigation strategies might be:

- Physical and technical; and
- Procedural or administrative
- Personnel based

Physical security and access control measures should be implemented and based on site-specific risk assessments. This may vary by site and depends on the production process point, but may include as feasible, segregated weighing and mixing areas with electronic access control to manage entry, lock and key control, cameras, door alarms, door logs, additional supervision, container security (e.g., locked partial ingredient storage), color-coded uniforms or bump caps to designate work area, and limiting personal items. This typically would include increasing the visibility of commodities during production and training the personnel to be aware of suspicious activity.

Other security measures which may help reduce vulnerability in mixing and weighing areas can include the following:

- There are significant inherent characteristics that would make access to the product very difficult (e.g., enclosed systems, pressurized equipment, railings, equipment safety features, or shields).
- The mixing or weighing process is under constant observation, or the view of the step is unobscured, preventing an inside attacker from adding a contaminant without being detected.
- There are numerous workers in the immediate area that would notice a contamination attempt by an inside attacker.
- It is extremely likely the inside attacker would be detected adding a contaminant to the food due to the need to conduct highly irregular or suspicious activities to contaminate the food; successful introduction of a contaminant at this point would be extremely difficult or impossible.

- Multiple workers are required to be present for the mixing or weighing procedure to function.
- Product is moving at a high rate of speed.
- Product is handled, staged, or moved in an inaccessible manner (e.g., bucket conveyors being moved via elevated track)
- These areas are staffed by permanent employees.
- All staff are instructed to systematically and immediately report any anomaly, unusual incident or behavior to their supervisor.
- Clear operating rules are defined in these areas.
- Access to change any sensitive parameter (e.g., access to recipes/formulae, key production parameters, release of products) and remote access (by supplier or operator) are secured by usernames and passwords.
- Tamperproof locking/sealing systems on ingredients or raw & direct food contact material containers, gases are systematically checked. Records are available. Corrective actions are taken in case of deviation.

Finally, operations personnel that work in the vicinity of the mixer/blending areas should have basic or general food defense awareness training that can support and drive future success of the site's food defense program.

Conveyance

Coming soon.

Batch Tanks

Coming soon.

Bulk Liquid Receiving / Storage

Coming soon

Ice/Water Processing Areas

Water is a critical element in most food and beverage manufacturing scenarios. As such, ice/water systems need to be secured as a critical part of the infrastructure. Examples of best practices include

- Restricting access to waters wells by lock or other access control methods.
- Restricting access to water storage tanks via locked ladder guards or locked tank hatches.
- Restricting access to water treatment systems and water softening processes where direct access to the water stream is a possible source of the introduction of a contaminant. .
- Establishing written agreements with water suppliers to notify the company immediately whenever they determine that the water supply has become unfit for use.

Bulk liquid receiving

Coming soon.

Liquid Storage

Liquid storage is a potentially vulnerable point for contamination. A contaminant added to a liquid storage tank could result in the blending of that contaminant into a product undetected. As such, liquid storage tanks need to be secured. Examples of best practices include

- Restricting access to liquid storage tanks via locked ladder guards or locked tank hatches.
- Alarming hatches so facility personnel are notified when there is access to a storage tank.

Finished product conveyance

Coming soon.

The ASIS Food Defense and Agriculture Security Steering Committee created this resource for the global food and beverage manufacturing community.
Originally published: November 2021

Important Procedural Matters

Visitor Management

Approval for visitors to access the facility should be obtained at least twenty-four hours in advance or at a minimum approved by a host. Visitors to the site should have to provide some form of official photo identification to validate identity. Ideally, visitors should enter via a separate entrance such that their movement and degree of access is limited controlled until being met by the host or escort. Visitors should always be escorted and only allowed access to areas where official business is conducted.

Whenever possible and not in contradiction to safety or good manufacturing practices (GMP), visitors should wear some form of identification which easily denotes their visitor status. This could include aa uniquely colored bump cap or color-coded vest indicating visitor status. Visitors should not generally be allowed into any area where manufacturing, products or ingredients are stored. A log should be maintained for no less than 60 days which contains information regarding the name of the visitor, the associated firm, the name of the escort(s)[1], areas visited and the time of their arrival and departure. An example of a visitor control log can be found in Appendix 1.

Truck Driver Management

Like visitors, truck driver access to the facility should be highly controlled. Truck drivers should not be allowed to enter any area of the facility where products or ingredients are manufactured or stored. When access to the facility is necessary to facilitate delivery or pickup of products, truck drivers should only be allowed to access the shipping or receiving area of the facility. Under no circumstances should truck drivers be allowed on the loading dock area, the manufacturing area or the storage area for products and ingredients.

Truck drivers may be instructed to stay in their cab during the unloading and loading process. Facilities might consider exterior portable toilets for truck drivers. Alternatively, sites may wish to provide a lounge for truck drivers. This lounge should be highly controlled to ensure that the drivers cannot access any other part of the facility.

Truck drivers should not apply or remove seals from trailers. Seals should be applied or removed by facility or security personnel. An example of seals management procedure can be found in Appendix 2.

A written or electronic log of truck drivers should be maintained for a period of not less than 60 days. This log should contain information regarding the name of the driver, the date and time when the driver accessed and departed the facility, and the name of the driver's employer.

Contractors/Temporary/Contingent Workers

Facilities should ensure that contractors who are "routine" or who frequently visit the site undergo a background screening process in line with personnel surety protocols for employees.

[1] For food defense plan record keeping purposes, monitoring and verification of escort practices.

The ASIS Food Defense and Agriculture Security Steering Committee created this resource for the global food and beverage manufacturing community.
Originally published: November 2021

Access to area(s) of the facility by contractors should be tightly controlled such that access is limited only to those areas needed to perform assigned tasks. When contractors will be performing work on site, consideration may be given to advising employees and supervisory personnel as to the nature, duration and location of the work.

Any access control badges and/or keys which are provided to contractors should be collected each day before departing the facility. Badges issued to contractors should be of a different design and/or color than those issued to employees or visitors.

Management and Storage of Partial Ingredients

In most cases, ingredients are received and stored in tamper evident packaging which allows for facility employees to detect tampering and contamination. However, in some cases, partial ingredient packaging may be present at a facility, and this is a potential point of vulnerability to contamination. Potential strategies to reduce the risk of contamination via partial ingredients include:

- Storage of partial ingredients in tamper evident containers (e.g., use of bins with numbered seals)
- Securing partial ingredients in locked storage
- Weighing partial ingredients returned to inventory and reweighing when next brought to mixing, weighing or staging steps in the production process

Finally, ingredient handlers should have basic or general food defense awareness training that can support and drive future success of the site's food defense program.

Hazardous Materials and Chemical Storage

From a product contamination perspective, a facility will likely contain non-food grade cleaning, sanitizing and facility equipment maintenance materials (that could be used as a contaminant) that are legitimately needed to support operations. Like lab security, cleaning and non-food grade materials must be protected from unauthorized access by a person intending on product contamination. Further, sound inventory control programs are another "layer" of protection assuring that these materials cannot be used for an act of contamination.

Physical security and access control measures for chemical and cleaning storage should be considered and implemented based on site-specific risk assessment. This may vary by site and depends on the lab's location in the facility. Common security measures might include electronic access control to manage entry, lock and key control, cameras, door alarms, door logs, additional supervision, container security (e.g., locked and potentially alarmed chemical storage), color-coded uniforms or bump caps to designate work area.

Fail-secure electronic locksets may be specified in non-food grade material storage situations to prevent unauthorized access to the facility if primary and backup power is lost. A fail-secure system requires power to unlock the door thus preventing circumventing of the security system by cutting power. Fail-secure locksets typically include key override to allow access by appropriate personnel in power outages. A door position switch can monitor door position for a variety of purposes and notify security personnel if it detects a door has been physically forced open or held open beyond the permissible time set in the software (e.g., 30 seconds).

Additional security measure should include maintaining a strict inventory and training. Appropriate personnel should always know where and how much hazardous materials are stored. Unaccounted loss of these materials should be reported immediately to security personnel and thoroughly investigated to determine the root cause and to determine if product has been impacted. Maintenance and sanitizing Personnel should be appropriately trained on security procedures and why they are important.

Non-food grade materials should never be left unattended in a production area and should be properly secured when not in use.

Finally, maintenance and sanitizing personnel should have basic or general food defense awareness training that can support and drive future success of the site's food defense program.

Restricting Personal Effects/Property from Production Areas

Coming Soon

Tamper Evident Solutions

Many manufacturers are required to develop and implement solutions for their products which meet the tamper-resistant standards as established by the governing regulatory agency. These solutions are intended to assure that the product's packaging can be reasonably be expected to provide visible evidence to consumers that tampering has occurred.

Tamper evident packaging on the other hand, is packaging which contains an indicator or barrier to entry which, if breached or missing, can be reasonably be expected to provide visible or audible evidence that tampering has occurred.

These solutions are important not just for final products, but also certain raw materials and other materials which are being blended during the manufacturing process. Implementation of these efforts reduces the possibility of intentional tampering/ adulteration.

Incoming Shipments

All trucks and trailers with supplies, raw materials, or finished goods must be sealed until use. If the seal must be removed for inspection, a new seal is applied and documented.

Unloading of vehicles transporting raw materials, finished products, ingredients or other materials used in food processing must be closely supervised. All supervisors must be trained in food defense procedures related to shipping and receiving.

Other than LTL and courier shipments, loading and unloading activities will be scheduled and/or monitored and only scheduled shipments will be accepted. Unscheduled or unauthorized shipments are held until authorization is obtained.

Only authorized personnel will be allowed access to the loading dock area.

Seals must be verified BEFORE the load is accepted.

Suppliers and Vendors

The risks associated with product tampering and intentional adulteration extend to suppliers of all products. As such, it is important that manufacturers know who they perform business with in order to ensure that a similar level of food defense planning is operational at those facilities as it is at the facility which manufacturers the final product. As such, consideration should be given to conducting security assessments of key product/packaging/raw material suppliers and vendors.

Physical and Technical Security

Perimeter Barriers

If a facility chooses to employ perimeter fencing, the following performance standards should be considered. Perimeter fencing is not a requirement of a food defense program.

Chain-link fencing should be at least 6 feet in height, excluding the anti-personnel climb guard. The fabric should be at least 9-gauge wire. This fencing should be galvanized with mesh openings not larger than 2 inches per side and have twisted selvages at the top and bottom. The wire should be taut and securely fastened to rigid metal or reinforced-concrete posts set in concrete. These posts should be evenly spaced to maintain fence tautness and strength. The top and bottom of the fence should contain a tension wire that runs horizontally along the entire fence line to help retain the integrity of the fence. The fencing must reach within two inches of hard ground or pavement. On soft ground consider extending below the surface to compensate for shifting soil or sand. Fencing would typically include a "top-guard" which is constructed of at least three strands of barbed wire placed at a 45-degree overhang that faces away from the property. The top guard should be continuous and not be omitted from vehicle or pedestrian gates. Top guard may need to be mounted vertically on such gates.

Walls should be at least 7 feet in height

Gates

Gates are the only moveable part of a fence and therefore should be properly constructed with appropriate fittings to ensure that vehicular or pedestrian access is controlled. Most vehicle gates are cantilever slide-like gates. Smaller gates limit the potential for vehicle piggybacking and can be closed quickly.

When employing pedestrian gates consideration of an access controlled self-closing mechanism is encouraged to prevent the gate from being left open.

Access Control

Access control is the process of restricting and/or controlling entry onto a property, a building, room, or other areas by means of physical barriers, key control, biometric/card pass systems or other electronic devices.

Entry devices and access control SOPs should be implemented to monitor and control access of authorized personnel and property into and out of locations while denying access to unauthorized persons. It is important that access control programs be properly managed to ensure that access to a facility and areas within the facility is granted by an individual with the appropriate level of authority to do so, access control can be attained via any combination of barriers, gates, electronic security equipment, and/or guards that can monitor and control entry and exit to a facility.

The objectives of an access control system are:

- To permit only authorized persons to enter the facility and select areas therein.
- To provide information to security personnel and/or site management for the assessment and response to unauthorized entry or attempts
- To detect and prevent the entry of contraband (e.g., weapons, contaminants, GMP violations) and
- To provide an accurate accountability of who has accessed the facility/area.

Lock and Key Control

The most important element of lock of key selection is choosing a keyway that is not easily duplicated without leadership approval. While there are limited product choices to meet this vital performance standard, the failure to properly select the right system will invalidate all other key control measures commonly used such as "DO NOT DUPLICATE" stamping, record keeping and audits. Ideally, each key should have a unique and generic number stamped on the key head which indicates which locks are accessible and the person to whom it is assigned. Designations such as "GM" for grand master should be avoided. A further description of common terms and guidelines can be found below:

Grand Master key: a key that typically operates all locks on site:

- This key should only be given to specific employees with a need for such access upon approval of Site Director and consistent with the facility's policy.
- Keys should not be issued based on title, but rather by need.
- In the case of electronic access control in use at a facility, the use of keys on card reader equipped doors should only be in an emergency.

Master Key: Typically, keys for multiple doors in a specific area.

- This key should only be given to specific employees with a need to access those areas.

Operating key: Typically, keys for office doors, work areas or specific locations.

- This key can only be given to specific employees with approval of the responsible person at that location.

Incidental Keys: Keys specific to an individual's workspace, (e.g., file cabinet keys, desk keys, safes)

All keys which are not issued should be stored in a secure location such as a locked container stored in an office that is locked after business hours. Examples include a locked metal box stored inside a locked office, or a lockable file cabinet inside a locked office.

Employees and select contractors can be issued keys. When issued, there should be a key control log maintained which captures which keys were issued to what employee on what date as well as when the keys were returned. The employee/contractor should sign for all keys which have been issued to verify receipt. Refer to Appendix 3 for a sample key control log.

Like Access Control badges, all keys which were issued to an employee/contractor should be retrieved prior to their off boarding. In the event a key is not recovered when a key holder separates from a company, a risk assessment should be conducted to determine the need for rekeying impacted areas of a facility. Minimizing key cylinders on the perimeter of a property and the perimeter of a building will reduce the likelihood of having to undergo an expensive rekeying project.

Video Surveillance

Video surveillance is a system in which an image is transmitted to monitors/recording and control equipment. Video surveillance should follow local legislation for both installation, signage, monitoring, training, recording access.

Fixed cameras are typically preferred over Pan-Tilt-Zoom (PTZ) Cameras. Whenever possible, cameras selected should provide the viewer with the ability to both monitor movement as well as identity. As an example, a fixed camera with wide angle view may be used to cover more than one turnstile, lane of traffic, or railroad track. In order to get facial recognition from a video image, the resolution needs to be at least forty pixels per foot in the target area of the scene.

Use color, day-night transition cameras where lighting is too low to render a good color image in hours of darkness.

15 frames per second might be considered for recording purposes or more where finer details may need to be observed when viewing recorded video.

There is no standard for video retention in the industry however a typical range is between thirty to sixty days. Retention for recorded video can vary by camera in an IP based system so careful consideration should be made for each camera as to the typical time it might take to discover an incident and then set the retention rates accordingly.

The strategy for camera deployment would typically involve access choke points (e.g., employee or vehicular entry points) or fixed monitoring on critical asset areas. However, it is not uncommon to find video surveillance cameras associated with the following areas:

- Car parks and lots used to store trailers and other equipment
- Administrative Offices
- Data Centers / IT Server Rooms
- Refreshment Areas
- Building exteriors

- The exterior and interior of loading dock areas
- The area where Quality Control testing is performed
- Dispensing and mixing areas.
- Locations where labels, coupons and anti-fake stickers are stored
- Packing lines – recommend one at one at each end
- Returned / Damaged Goods areas
- Waste Processing Areas
- Other identified Critical Control/High Hygiene areas within the manufacturing areas
- Areas where controlled and/or listed chemicals are stored
- Area where hazardous materials are stored
- Perimeter fence

Cameras should only be deployed after a risk assessment and consistent with where video can have a meaningful impact on risk reduction. Consider the use of an independent expert to help identify these needs rather than a company that sells video equipment that may have a conflict of interest in any recommendations made.

Intrusion Detection

Intrusion detection System (IDS) is a system that uses a sensor(s) to detect an impending or actual security breach and to initiate an alarm or notification of the event. Alarm response can be managed internally, by a 3rd party alarm response firm or law enforcement. The primary objectives of an IDS are:

- Detect an actual or attempted intrusion into a protected space or removal of assets from a protected space;
- Provide protection in depth to the facilities, buildings, assets, and operations to be protected, enabling corrective assessment and response;
- Meet the needs of the application, integration with other physical security systems to provide protection in depth;
- Facilitate security response by pinpointing where an intrusion has occurred and possibly where the intruder has moved;

Strategies for the effective management of an IDS include:

- Train employees on the proper arming and disarming protocols to reduce nuisance alarms and costly municipal charges
- Ensure employees know the protocols to follow in the event of an accident system activation
- Do not allow multiple persons to share a code
- Test the system regularly
- Ensure there is battery back up to sustain protection in a power outage
- Consider the need to enhanced monitoring and reporting which might include:
    - Failure to open
    - Failure to close
    - Monthly review of openings and closing
- Regularly update names and persons contacted in the event of an alarm activation.

The ASIS Food Defense and Agriculture Security Steering Committee created this resource for the global food and beverage manufacturing community.
Originally published: November 2021

- Do ask employees to respond to alarms alone. No facility entry should be made by anyone other than a law enforcement officer.

Personnel Identification Strategies

As previously mentioned, access to manufacturing, raw ingredient and product storage areas of the facility must be highly controlled. In addition to access control procedures, consideration should be given to developing mechanisms to visually identify the status of personnel on site. This can be accomplished by a variety of means include color coding of access badges, clothing or bump caps.

Entry and Egress Openings

Keep pedestrian doors on the ground floor under surveillance (manned or otherwise) during working hours and locked out of working hours.

- Consider installing card access or biometric access enabled turnstiles to confirm only authorized staff will enter.
- Keep access to loading bays and delivery chambers closed except for deliveries and dispatching.
- If kept open for ventilation (and this is typically not a recommended practice), avoid flimsy bug screens which can easily be breached by an unauthorized person by lifting the base or cutting through the screen mesh.
- Secure all ground floor windows with bars or metal shutters where possible. Keep all windows closed unless someone is present in the room.
- Improve the sturdiness of any roof openings (e.g., fanlight, vents) and ensure that they are alarmed/locked.
- Keep roof access under video surveillance

Emergency Exits

- Keep emergency doors locked from the outside, free egress from the inside.
- Remove all exterior hardware from emergency man doors.
- Do not allow key cylinders to be installed on emergency exits and blank them out if they already are.
- Emergency exits should be alarmed on a twenty-four-hour basis (not just when the IDS is armed) such that when opened an alarm is sent to a central receiving alarm monitoring station, either internal or external.
- Consider the use of local audible alarms to deter the use of doors.
- Consider the application of numbered seals as an added assurance that an exit door has not been used.

Personnel Matters

Personnel Surety

According to ASIS, "Employers from the largest to the smallest, understand the dual benefits of hiring the best people and providing a safe and secure workplace – both physically and financially – for their employees, customers, shareholders, and the community in which they operate. A key factor is to know as much as you can about the people you want to hire and to know that before hiring them. Hiring a new employee is an important responsibility for any organization. An employer who has performed a thorough preemployment background screening on its applicants is more likely to bring into the organization a highly skilled person who will prove to be a tremendous asset. Unfortunately, absent a sufficient pre-employment background screening, that same employer runs the risk of exposing his or her organization to someone who could ultimately become the organization's greatest liability." (ASIS International, GDL-PBS-2009, 2009, p. 1).

This is a critical mitigation strategy for the food and beverage industry given the preponderance of the threat is born from insiders. In essence, personnel surety is about ensuring trusted persons are in fact trustworthy. Background checks are almost universally addressed when one looks at various global models.

For example, as part of the FDA Food Safety Modernization Act (FSMA), the Food and Drug Administration (FDA) issued on May 27, 2016, a final rule to require domestic and foreign food facilities, with some exceptions, to address hazards that may be introduced to food with the intent to cause wide-scale harm to public health. These food facilities are required to identify significant vulnerabilities and take steps to minimize or prevent them. § 121.130 Vulnerability assessment to identify significant vulnerabilities and actionable process steps, subsection (b) states, "The assessment must consider the possibility of an inside attacker" (https://www.ecfr.gov/current/title-21/chapter-I/subchapter-B/part-121).

Another example can be found in the UK's Food Standard Agency's PAS 96: 217 "Guide to protecting and defending food and drink from deliberate attack" in section 2.9 which reads, "Personnel Security – procedures used to confirm an individual's identity, qualifications, experience and right to work, and to monitor conduct as an employee or contractor." The definition is footnoted with the following, "Personnel security principles are used to assure the trustworthiness of staff inside an organization but may be applied to the staff of suppliers within processes for vendor accreditation." The document further goes onto discuss this topic by adding, "Personnel security guidance is used to mitigate the insider threat to the organization. Its principles can also be used by food businesses to judge whether key staff within the organizations that supply goods and services can be trusted to comply with specifications and procedures, and to work in the best interest of both the supplier and customer.

Insider attacks against the food supply aren't limited to acts of terrorism and can be perpetrated by employees, contractors or suppliers, essentially anyone with access to the facility; therefore, it is critical for every organization to improve its ability to identify an inside attacker.

The following is a list of generally accepted means by which personnel surety or security for candidates and on an ongoing basis with insiders might be achieved through the following verification activities:

- New Hires
    - Identity
    - Eligibility to work in the host country

The ASIS Food Defense and Agriculture Security Steering Committee created this resource for the global food and beverage manufacturing community.
Originally published: November 2021

    - Qualifications, experience and past performance
    - Establishing and monitoring to ensure contract employees who may be unescorted or work in sensitive areas are vetted by employers with the same standard and company employees
    - Suitability (from a criminal background check and in keeping with human resources best practices such as the whole person rule)
    - Drug testing which is complicated by legalization trends
- Ongoing Personnel Surety or Security
    - Limit new employees, contractors or temporary employees in highly sensitive process areas
    - Monitoring and supervision
    - Confidential reporting and whistle blowing mechanisms
    - Knowing who is and who should be on premises, and where they should be located, for each shift keeping assignment information updated
    - Establishing a system of positive identification and recognition that is appropriate to the nature of the workforce (e.g., issuing uniforms, name tags, or photo identification badges with individual control numbers, color coded by area of authorized access)
    - Identifying staff that require unlimited access to all areas of the facility and limiting others accordingly. Reassessing access privileges regularly.
    - Limiting access so staff enter only those areas necessary for their job functions and only during appropriate work hours (e.g., using electronic access control systems)
    - Restricting the type of personal items allowed in non-public areas

Refer to the section entitled, "Change Management" for additional relevant information.

Security Awareness and Food Defense Training

Security awareness programs promote compliance with security policies and procedures which are intended to guide individual and organizational behaviors and attitudes. Properly developed awareness programs articulate management expectations, security guidance and provide information regarding where to go for additional tools and training. Effective security awareness programs are part of on-boarding and retraining processes and are regularly reviewed and updated. Key attributes of mature security awareness programs include, but are not limited to the following:

- Top-down management support and emphasis
- Mechanisms for individuals to report security concerns/violations
- Continuous review to maintain relevancy
- Realistic training content which provides a clear picture of risks and responsibilities
- Recurring training to keep security and food defense on top oof mind with all key people

For the food and beverage facility, food defense training is a subset of the overall security awareness training mission and a critical one. In every organization, leaders, security and food defense professionals must take stock in the threats and resulting risks to the organization. Arguably, just because an organization produces a food or beverage product, that organization is no less subject to workplace violence events. Therefore, when mapping out the needs to elevate employee security and food defense awareness the training needs to be comprehensive and thorough. Food and beverage manufacturers should not limit training to food defense only and programs should include all these key attributes and include not only internal, but also external guidance and best practices as supplied by reputable regulatory and academic institutions.

Food Defense Training Sources

There are several sources of food defense training, some of which are focused on the US based Intentional Adulteration Rule.

- https://www.fda.gov/food/food-defense-tools-educational-materials/food-defense-101-front-line-employee
- https://www.ifsh.iit.edu/fspca/courses/intentional-adulteration

Some of the audiences that should be considered in any food defense program would include but in no way be limited to:

- Senior facility leadership
- Food defense team
- Qualified individuals who will perform vulnerability assessments, write food defense plans and steward the reanalysis and compliance maintenance
- Persons working at actionable process steps and the supervisors of those persons
- Persons dealing with contractors (to ensure contraband is not allowed in the facility)
- Persons managing visitors (to ensure that they are vetted and escorted)
- Persons handling chemicals and sanitation materials
- Persons interfacing with truck drivers in a receiving and shipping capacity

Additional guidance to establish and sustain effective security awareness programs can be found within ASIS Standard ASIS SA-2020, Security Awareness, with the caveat that one needs to be a member of ASIS to access this document.

Peer Monitoring

Concept of Natural Surveillance

Natural surveillance limits the opportunity for crime by taking steps to increase the perception that people can be seen. Natural surveillance occurs by designing the placement of physical features, activities and people in such a way as to maximize visibility and foster positive social interaction.
Natural surveillance includes the placement of windows and open areas with clear lines of sight. Natural surveillance also refers to activities that have a relatively high number of people in the area for the designated function or activity.

Security Integrity Assurance

Security Challenge Testing (Physical Penetration Test)

Food defense programs can undergo continuous improvement when individual mitigation strategies are regularly verified. A common means to verify the effectiveness of your physical security program is called a security challenge test (CT). An effective security challenge test program might include:

- Conducting regularly scheduled tests
- Sharing the results with the workforce to increase security awareness. For instance, if a challenge test results in a security breach, reminding employees or proper procedures for follow. In the event the challenge test does not result in a security breach a positive communication might be considered for the workforce celebrating the positive effort.
- If a challenge test results in a security breach, a facility might consider retraining and executing a similar test to assess whether the identified vulnerability has been resolved.
- A facility may also consider documenting the results of security challenge testing which may illustrate lessons from which other facilities in an enterprise may benefit.

When a security challenge test is conducted, it results in one of two outcomes; 1) Pass (security breach attempt detected and proper response by person or system); or 2) Fail (security breach attempts not detected and improper response by person or system).

Guidelines for executing tests:

- CT's might be conducted quarterly for plants and company headquarters.
- CT's might be conducted semi-annually for offices and DC's.
- Do not endanger the safety of individuals.
- Do not disrupt business or operations.
- Dependent upon the test scenario, consider informing local law enforcement that security challenge tests are taking place, especially if a test is carried out at night.
- Do not undertake any illegal activity.
- Do not record an actual incident / occurrence as a security challenge test. Observed unplanned events would be logged as security incidents or near misses.

Physical Security and Security Systems Maintenance, Inspection and Testing

Physical security measures should be regularly calibrated, maintained and tested. Recommendations for such a program would include:

- Develop a master list of all systems to include calibration, maintained and testing required to include a frequency.
- Assign responsibility.
- Track.
- Create records to demonstrate what work has been done.

Change Management

Coming Soon

Appendices

Appendix 1 – Food Defense Resources

Food Defense Resource Description	Link
A Food Defense Resource Center has been established which contains presentations, white papers and articles relevant to food defense.	https://foodsafetytech.com/food-defense/
The Food Defense Mitigation Strategies Database (FDMSD) is a tool designed to help owners and operators of a food facility with identifying mitigation strategies to protect the food against intentional adulteration, and may assist them with meeting some requirements of the Mitigation Strategies to Prevent Food Against Intentional Adulteration regulation (21 CFR Part 121).	https://www.cfsanappsexternal.fda.gov/scripts/fooddefensemitigationstrategies/index.cfm

Appendix 2 – Visitor Management Terms, Conditions and Log

You are requesting entrance to a facility owned and/or operated by our company ("Company"). We welcome you but remind you that, in consideration for your admission, you are agreeing to abide by our Company rules and the terms stated below which apply to any facility owned and/or operated by Company or its affiliated companies or divisions.

Respect for Company Procedures & Law - You agree to comply with the Company's safety, security, environmental and health procedures including, but not limited to: Standards of Business Conduct, Drug Free Workplace & Substance Abuse Policy and health & safety policies while on the premises of any facility owned or operated by Company or its affiliated companies or divisions. Copies of our policies are available upon request but, in general, visitors are expected to (i) respect our employees and our corporate property and assets, (ii) conduct themselves and their business in a safe and courteous manner, and (iii) abide by applicable laws.

No Photography or Recordings - You understand that audio/visual recording or photography on any device (including cell phones) is strictly prohibited unless express written permission is obtained from an authorized Company representative. This prohibition applies not only within any Company facility but also to any meeting with Company representatives or to any Company equipment or materials.

Good Manufacturing Practices (GMP) – By using this form, you are acknowledging that you have been provided, understand and agree to abide by company operations, GMP and safety rules.

Respect for Confidential Information – You understand that this facility and the equipment and materials within it constitute Company property and are of a private and proprietary nature. You agree that you will not, directly or indirectly, record, remove, use or disclose to others any Company Confidential Information. "Company Confidential Information" means all information not generally known to the public that you observe or receive in connection with any facility visit (including information communicated to you in anticipation of, or as a follow-up to, your visit). Company Confidential Information specifically includes, but is not limited to, all of the following: ideas, inventions, products, prototypes, designs, drawings, plant/facility layouts, manufacturing equipment, processes and techniques, customer and supplier information, blue prints, distribution techniques and systems, pricing information, formulations, ingredients, specifications, know-how, testing procedures and results, as well as advertising and marketing materials, business plans, forecasts, budgets, costs and financial information and employee information.

BY ENTERING OUR FACILITY, YOU AGREE TO FULLY COMPLY WITH THESE TERMS AS ACKNOWLEDGED BY YOUR SIGNATURE BELOW.

Visitor Name	Visitor Signature	Date	Time In	Time Out	Host (Person visited)	Host Signature	Escort Required (Y/N)	Badge # Issued
*I have carefully read and understand the terms of the **Visitor Agreement** posted at the check-in desk and agree to comply with those terms during this and any other visit to a facility owned by the Company or its affiliated companies or divisions. I understand these obligations carry on after my visit.*								

858
859

Appendix 3 – Seal Management Protocol

Coming Soon.

The ASIS Food Defense and Agriculture Security Steering Committee created this resource for the global food and beverage manufacturing community.
Originally published: November 2021

Appendix 4 – Key Request Form

KEY REQUEST FORM

(Use one form for each key only)

NAME_____

EMPLOYEE ID#_____PHONE/EXT. #_____

KEY#_____ KEY SYMBOL_____ COPY#_____MFGR_____

KEY LOCATION(S)_____

_____

Key Issue Agreement: In return for the loan of this key, I agree: **1)** not to give or loan the key to others; **2)** not to make any attempts to copy, alter, duplicate, or reproduce the key; **3)** to use the key for authorized purposes only; **4)** to safeguard and store the key securely; **5)** to immediately report any lost or stolen keys; **6)** produce or surrender the key upon official request. I also agree that if the key is lost, stolen, or not surrendered when requested a charge that reflects the cost of changing any and all locks affected may be assessed.

SIGNATURE_____ DATE_____

DEPOSIT (if required) _____ ISSUE TYPE: STANDARD ☐ TEMPORARY ☐ REISSUE ☐

DUE DATE_____ REASON_____

AUTHORIZER'S SIGNATURE_____DATE_____

PRINTED NAME_____

TITLE_____

PHONE_____

OFFICIAL USE ONLY

DATE ISSUED_____

BY_____

CONTROL #_____

ENTERED BY_____

KEY RETURN:

RETURN DATE_____**BY**_____

RETURN REASON_____

_____

DEPOSIT RETURN_____

KEY NOT RETURNED:

☐ LOST ☐STOLEN ☐BROKEN ☐OTHER

EXPLAIN CIRCUMSTANCES:_____

_____

_____

_____

SIGNATURE RECEIPT_____

The ASIS Food Defense and Agriculture Security Steering Committee created this resource for the global food and beverage manufacturing community.
Originally published: November 2021

Appendix 5 – Key Temporary Sign Out/In Tracking Log

Name of person receiving key	Key Area	Date	Time Issued	Time Returned	Issuer Name

The ASIS Food Defense and Agriculture Security Steering Committee created this resource for the global food and beverage manufacturing community.
Originally published: November 2021