



International Dairy Foods Association
Milk Industry Foundation
National Cheese Institute
International Ice Cream Association

BIOSECURITY IN THE DAIRY PLANT **IDFA's Guidance Document for the Dairy Industry**

This guidance document was prepared by the International Dairy Foods Association (IDFA) to help you evaluate the security and integrity of your operations in dealing with a deliberate act of tampering - however unlikely. Our industry has long dealt with issues of food pathogens and inadvertent adulteration; we now need to review our systems with a new perspective.

Each plant has its own handling protocols, physical lay-out and employee policies. Therefore, this document is not all-inclusive, but should help you review your operations to see if changes are needed. Please use this paper to stimulate your thinking and planning. IDFA urges all members to seek consultation from experts to address any specific issues of concern in your plant.

We have laid out areas to consider in order of milk and other materials entering your facilities, through to the distribution of finished product.

I. Incoming Materials

In general, start by considering the milk, food ingredients, packaging, chemicals and other materials that come into your plant facility and warehouses, and ensure that these product streams are secure, and that materials are stored in a secure place.

A. Milk Tankers

- Consider the security of your tanker trucks that transport milk, cream and other liquid bulk products. Consider their movement from farm to farm, or plant to plant, as well as parking and off-hours holding, and unloading and cleaning for re-use. Is the truck secure from tampering at all times?
- Trucks should not be left unlocked and unattended, whether full or empty.
- Regardless of where the truck is parked (within view or out of sight) nobody should have access to the inside of the tanker unless they are unloading or cleaning it.
- Consider ways to tag or lock the bulk area of your trucks for tamper-resistance or tamper-evidence at each step of the journey.
- Raw milk suppliers should provide information on driver identification, driver background checks and measures taken to assure that potential food safety issues are addressed and controlled.

- Your receiving people should be able to identify the truck driver, to be sure that he is who he says he is. This could be as simple as having the driver register with your office and confirmed with a phone call. A picture I.D. can be used for verification.
- Discuss these issues with your hauler and maintenance staff to determine the easiest and most effective way to accomplish these important precautions.

B. Other Incoming Materials

- Consider the trucks that carry all of your supplies to your plant - packaging, ingredients, etc. - and apply the same consideration for these trucks as the milk tankers above. Consider a tagging system with your suppliers that ensures these materials have not been tampered with in-transit.
- Compile documentation from ingredient and packaging suppliers on their safety and security programs.
- Reconcile the amount of ingredient received with the amount ordered and the amount listed on the invoice and shipping documents.
- Supervise off-loading of incoming ingredients, compressed gas, packaging, labels, salvage products, rework products, and product returns.
- Keep inventory of ingredients, packaging, labels, salvage products, rework products, and product returns.
- Investigate missing or extra stock or other irregularities outside a pre-determined normal range of variability and report any unresolved problems to local law enforcement.
- Destroy outdated or discarded product labels to prevent product counterfeiting.
- Some liquid bulk ingredients are pumped into the plant through inlets on the outside of the plant. These should be secure.
- Bagged dry ingredients (nonfat dry milk, spices, etc.) should be in bags that show no evidence of tampering. Half-full bags should have the name of the operator who last used it and the date it was last used written on the bag. Half-full bags should be stored in a secure place.
- If your water supply is from a public works facility, check with city officials to find out what security measures they have in place. If you use a private well, secure it.
- Consider the storage of your ammonia and other chemicals, and ensure that these materials are secure.

C. Security in the Receiving Bay

- The receiving bay can be a point of vulnerability. If your bay is big enough, the roll-down door should be closed after trucks are inside and positioned for unloading. If the bay is not big enough to do this, or if your bay has no door, you should train your receiving operators to watch for anyone who tries to get into the receiving area.
- The door leading into the plant should have a keypad or some other device that restricts entry.

- Pumps and other equipment in the receiving area should be secured from tampering. Sample plugs (the in-line rubber device used to pull samples) should be installed in a protected location where they can be observed.

II. General Plant Security

Consider the perimeter of your facility, entrance and egress to your plant and warehouses, access to all storage areas, and security of key areas within the plant.

A. Plant Perimeter/Interior Security

- Consider the perimeter of your plant. Do you have appropriate fencing, gates and/or surveillance to deter trespassers?
- Is outside lighting adequate?
- Security plans should be in place for weekends and holidays.
- Secure access to air intake points for the facility, to the extent possible (e.g. fences, sensors, guards, video surveillance).
- Routinely examine air intake points for physical integrity.
- Restrict Access to areas where chemicals (e.g. ammonia, sanitizers pesticides, etc.) are stored and make sure a supervisor monitors who goes in and out.
- Ladders on outdoor silos should be locked so that nobody can get to the top hatch. All points that allow access to the inside of the silo should be locked or somehow secured.
- All doors and windows that allow access to the plant need to be secured. Most windows and some doors can be locked more-or-less permanently. Other doors need a keypad or some other security device to restrict entry. *Be careful to keep within the fire code.*
- If you have doors that are not necessary, shut them permanently. Again, remember the fire code.
- Computer access to production records should be password protected.
- Eliminate computer access to past employees immediately upon voluntary or involuntary termination.
- Establish a system of traceability of computer transactions.
- Review adequacy of procedures for backing up critical computer-based data systems.
- Some silo bays have doors that allow access both from the plant and from the outside. It is very important to put keypads on all of these doors.

B. Processing Areas

- Maintain the safety and security of processing equipment through cleaning records, employee traffic and access control.
- Limit access to sensitive areas of your operation. For example, areas on the processing floor that have bulk holding tanks (silos, staging tanks, etc.) should have restricted access, if possible. Painted lines on the floor may be useful to identify such areas.
- Be sure that procedures and documentation for processing rework are in place and followed.

- Laboratory reagents should remain in the lab except when needed for sampling, etc.

III. Personnel

Consider all personnel movements within your plant, and in and out of your plant, including management of temporary employees and guests. Communicate with your people: Remember that your plant employees are your first (and best) line of defense against intentional contamination of your products. Enlist them in helping identify any suspicious people in or around the plant. If you have just 50 employees, you will have 50 sets of eyes and ears looking out for the safety of your products 24 hours a day, seven days a week.

A. Employee Access

- Consider performing citizenship, immigration status and criminal background checks on all employees.
- Review your hiring procedures: check the references for any new employees, and make background checks as appropriate.
- If an outside hiring source is used, verify that their recruitment methods are acceptable.
- Train all employees in your security procedures (including temporary workers) and enforce these policies.
- Change combinations and or collect the retired key card when an employee is terminated, either voluntarily or involuntarily, and additionally as needed to maintain security.
- Prohibit personal items (e.g. lunch containers, purses) in food handling areas (e.g. eliminate pockets from uniforms).
- Establish policy and provide for inspection of contents of employee lockers (e.g. metal mesh lockers, company-provided locks), bags, and vehicles when on company property.
- Consider color coding employee clothing so that it is easy to spot if people are in a restricted area. This might be particularly helpful with temporary employees who might not be allowed near certain areas.
- Casual laborers should be restricted to designated areas. This is important, as you often do not have background information on these people. Put one of your better Production Managers in charge of these temporary workers.
- Be aware of unusual behavior by plant personnel such as arriving early or leaving late, accessing restricted files or removing files.
- Storage facilities for employees (e.g. lockers) should be secured with company owned locks. Company procedures should permit access to these areas.
- Account for all keys to the facility.

B. Visitors and Vendors/General Surveillance

- Review or establish a sign-in procedure for visitors. Any vendors and other visitors should sign in and have an escort during their time in the plant. If a

vendor representative is unfamiliar to you, call the vendor to verify that they are who they say they are. Visitors should present a photo I.D.

- Consider requiring visitors, temporary employees and vendors to wear identifying clothing during their time in the plant.
- Security cameras positioned at strategic points around the plant and monitored at a central location can provide excellent protection against intruders.
- If you don't currently have one, consider an electronic security system that requires a magnetic card for entry.

IV. Distribution

A. Final Product Distribution

- When a truck carrying your products has multiple stops, the truck should be sealed with a tamper-evident device until the first stop, and locked when the driver is away.
- Truck drivers who distribute your product should be enlisted to watch for suspicious activity around the truck during stops.
- Ensure that public storage warehousing and shipping (vehicles and vessels) practice appropriate security measures (e.g. include requirements in contracts and audits).
- Perform random inspection of storage facilities, vehicles, and vessels.
- Advise sales staff to be on the lookout for counterfeit products during visits to customers and report any problems to management.
- Maintain records of product distribution, including product code (i.e. lot number) and consignee.

V. Crisis Planning

A. Planning/Authorities

- Have a crisis plan in place for your facility.
- Have tested recall programs in place in all plants in the event of a recall.
- Maintain floor and flow plan in secure, off-site location with local fire officials.
- Discuss emergency plans with police/fire/rescue officials so that their questions about the physical facility and materials/chemicals stored in it can be answered.
- Designate an emergency management coordinator and back-up for each processing plant, available 24/7. This person would be responsible for receiving any emergency or safety concerns, documenting their receipt, making contact with the corporate offices, determining the significance of the information, and notifying IDFA and the government agencies, as necessary.
- Educate your employees as appropriate on your plan, and on the need for vigilance in food operations.
- Contact your local police and let them know that you have implemented security plans. Meet with a local law enforcement representative on site and show him your plans.
- Make sure the local police and fire department have contact phone numbers for your facility so that you can be contacted 24 hours a day, 7 days a week. Be sure

that your employees have phone numbers for the police, sheriff and fire department in case they need to report an incident.

- Designate and train a media spokesperson.
- Prepare generic press statements and background information.
- Annually review and test the effectiveness of procedures and plans (e.g. mock criminal, terrorist or tampering events, mock recall) and revise accordingly. Use third party or in-house security expert.
- The Food and Drug Administration (FDA) has an emergency operations telephone number you can call in case of an incident. The number is (301) 443-1240. Keep this number close by.
- IDFA's emergency contact is Cary Frye at 202-220-3543 or 202-841-0062 (cell phone); or Allen Sayler at 202-220-3544 or 202-841-1029 (cell phone).

If you have additional questions about plant biosecurity, call Cary Frye or Allen Sayler at (202) 737-4332.