"Seal-Tite" Program

Milk Truck Security Measures for British Columbia

Management and Training Manual

Developed for the

B.C. Milk Marketing Board

Table of Contents

A. The *"Seal-Tite"* Program

1. Introduction

Anyone who receives food products wants them to be safe, wholesome and secure from tampering. In the past, the industry's reputation and verbal assertions on their level of commitment was sufficient to maintain customer trust. However, with recent events, today's buyers want and need more.

The goal of the ***Seal-Tite Program*** is to begin the process of increasing awareness of potential security risks and set standards of equipment and methods to reduce these risks. No transporter will be able to protect itself against all possible risks. Reducing risk, however, can be achieved by anticipating or recognizing risks in the day-to-day operation and intervening where possible to decrease the risk to an acceptable level.

Through the BC Milk Marketing Board's initiative, a Technical Writing Team was assembled:

- Steve Islaub, Vedder Transport;
- Myron Glatt, Agrifoods International Cooperative Ltd.;
- Warren Penner, B.C. Milk Marketing Board;
- Tom Demma, B.C. Milk Marketing Board; and,
- Annette Moore, Quality First in Agriculture Inc.

The team researched and developed the protocol and assessment forms provided within this guide.

The program outlines the Best Management Practices (BMPs) that have been identified to be essential to the program. **Shaded areas within the document identify areas that are <u>mandatory</u> for a transporter to be recognized under the *Seal-Tite* Program.** All others are recommended best management practices and should be considered for future implementation.

Seal-Tite is a HACCP-based Program

Development of this program used the basic principles of HACCP. HACCP (pronounced has-sip) is a practical approach that identifies hazards (biological, physical and chemical) and determines critical areas where preventative steps can be taken to eliminate or minimize risk. HACCP is a systematic and preventive approach to achieve food safety standards. Originally developed in the United States to guarantee the safety of astronauts' food in space, HACCP is now being adopted worldwide as a scientific, straightforward and effective approach to enhance food safety.

By incorporating simple steps into the daily activities, hazards can be reduced or stopped. Documentation (e.g. simple checklists, standard operating procedures and records) will ensure that key proven steps are not forgotten or altered. Also, by tracking what gets done, where, when and by whom, corrective actions can be taken to remedy any problems and the whole program can be evaluated to make sure the situation is not repeated. To maintain a HACCP-based program you:

- Say what you do,
- Do what you say,
- Prove it, and,
- Change it, wherever necessary.

Implementing proven ***Best Management Practices*** (BMPs) and procedures, monitoring implementation and verifying key steps can improve food safety and security. BMPs are the foundation of any HACCP-based program. The ***Seal-Tite*** program has determined three BMP areas:

1. Tanker Security
2. Communications
3. Incident Response

Within these three areas the management practices were reviewed and standard operating procedures and related record keeping were developed to minimize the risk of tampering and increase overall awareness and security of milk. The minimum life span of any record is typically the time between audits, but may be extended depending on product shelf life. Everyone involved (e.g. drivers, wash personnel, dispatch, management and administration) must monitor and control these BMPs by using a combination of records:

- **Permanent Records** are where data is collected in a tabular format for easy identification, recall and evaluation.
- **Standard Operating Procedures (SOPs)** are written step-by-step instructions describing how a certain procedure is to be done (e.g. placement of seals). By establishing SOPs everyone understands how to do the job consistently and thoroughly.
- **Emergency Plan** outlines what staff should do if something goes wrong. People know, before it happens, what to do, reducing confusion and risk.
- **Checklists** are designed as a means to evaluate the operation in the beginning to determine current level of compliance and to use on a regular basis to monitor how well the program is being maintained. Drivers may see that what is considered an acceptable risk this year, many not be an acceptable risk next year. **(Record#4-Security Review).**

Other documents management should be aware of for development, implementation and training of the program:

- Seal-Tite Program - TMR Manual

2. Training

Orientation of New Employees

Often new staff is reluctant to ask too many questions at the start of a job for fear of embarrassment. By providing them with an orientation, you give them a chance to:

- learn what you expect from them
- understand the methods and “tools” of the operation and it’s programs (e.g. Seal-Tite), and
- appreciate the importance of their role in maintaining security.

To do this, consider providing them with a;

- list of written explanation of their tasks (e.g. SOP on Seal Placement), responsibilities and workplace policies that relate to the Seal-Tite Program
- tour the facility to explain the security requirements of your operation
- map — (especially if supplies are scattered in a number of different areas)

Staff Training

Training has two major benefits:

1. Improved productivity and quality, because trained staff will:
   - do the right thing the right way
   - waste less time and materials
   - offer new and better methods of doing things.
2. Improved motivation and job satisfaction, because training and ongoing managerial support will help staff meet new challenges.

Even the best-planned program will not work unless staff understands the principles and practices.

Training helps staff learn:

- **who** does what
- **what** the rules ,policies and standard operating procedures are
- **when** the SOPs and records are to be implemented
- **why** it is important
- **where** the critical areas are.

The Training Process

- √ **Develop a training plan**. Work with your staff to develop an implementation plan for your operation. Get their input on the practices, corrective measures, standard operating procedures and record-keeping responsibilities.
- √ **Set objectives.** Clearly state the specific tasks each employee should be able to do after training.
- √ **Select training methods.** Training should progress from basic to complex in small, easy-to-master steps. Match the training method, including whether to provide individual or group instruction, to your employees' skill levels.
- √ **Use the four-step method (Table 1) of Prepare, Present, Try out, Follow-up.** Active involvement promotes learning: we learn by doing.
- √ **Evaluate the training**. Have the objectives been met? How does staff feel? What are the 'bottom line' results or benefits? Are SOPs being practiced? Are records being kept? Are security indicators improving?

Table 1. The Four-Step Method of Training

Step 1 — Prepare	**Step 2 — Present the operation**
• Put the learner at ease. • Find out what he or she already knows about the job. • Get him or her interested in learning the job. • Place him or her in the correct position.	• Tell, show, illustrate and question carefully and patiently. • Stress key points. • Instruct clearly and competently, one point at a time — but no more than the learner can master.
Step 3 — Try out performance	**Step 4 — Follow up**
• Test by having the learner perform the job. Have him or her tell and show you and explain key points. • Ask questions and correct errors. • Continue until you are satisfied that he or she knows the job.	• Put the learner on his or her own. • Check frequently. Designate someone who can help if needed. Get the learner to look for key points as he or she progresses. • Taper off extra coaching and close follow-up.

3. "Team" Requirement of the Seal-Tite Program

A successful security program includes everyone! It is not meant to be a management program only, but a working document with input and "buy-in" by all staff. For a security program to work, it is critical that:

- **Implementation steps are clear** - everyone, (e.g., drivers, washers, external and internal security staff, management, mechanics, cleaning staff) is involved in the implementation and adjustment process. By incorporating ownership and describing the benefits of implementation greater success will be achieved.

- **Establish accountability** - Be clear on accountability. Identify who is responsible for implementation and assemble a team with representation from each section. To be successful, management must be behind the control measures put in place and provide support and solutions when deficiencies are noted. Prior to implementing a control measure ensure there is approval at all levels. Most failures with risk control are driven by the failure to properly involve personnel impacted by the risk control.

- **Promote support.** Develop the best possible supporting tools and guides to help with implementation, such as standard operating procedures for safety and security. The easier the task the greater the chance for success. Be sure to identify reasonable timelines for implementing. To be fully effective, risk controls must be sustained. This means maintaining the responsibility and accountability for the long haul. Provide management support and positive motivation with incentives for promoting and supporting food safety and security. Consider establishing contact with the local authorities and upper management (e.g. human resource experts, fire, and police) so they are aware of the program requirements. Not only do you achieve their support, but you will also receive valuable feedback on any parameters that may not agree with local by-laws or company policies.

- **Follow through.** Risk control programs fail when document control is not maintained and identified problems are not acted upon. Always follow up whenever a procedural change occurs to ensure the posted protocols and records match. If at any time a problem is noted and a corrective action is required, it is essential that it be accomplished within the designated time. If this is not done, the message to staff will be "it's not important" and the program will fail.

To ensure a functioning program the following practices must be in place:

- Identify critical areas/points within each operation (e.g. after washing the tanker) and establish control limits for each (e.g. place seals on all milk contact access points).
- Establish ongoing monitoring requirements unique to your operation for each of the critical areas to determine:
  - Who will check it?
  - What will be checked?
  - How it will be measured.
  - How often it will be checked.
- Allow only trained authorized personnel to be in control of these areas.
- Take corrective action if a problem is noted.
- Verify that monitoring is happening (i.e. check the checker), using management or technical personnel.
- Keep accurate records.

4. Understanding the Aggressor

To prevent tampering at any level it helps to understand the types of aggressor and the likelihood of attacks. There are five primary types of aggressor: criminals, protesters, terrorists, subversives and rogue or disgruntled insiders.

Tactics Used by Aggressors

Attacks can be expected to come in four common themes:

- Exterior attacks from outside the facility.
- Forced entry by creating a new opening in the facility in order to gain access.
- Covert entry by, using deception or stealth in order to gain access to materials, food, air or water systems.
- Insider compromise, using someone with legitimate access.

Agents Used by Aggressors

- **Biological** agents (bacteria, toxins, viruses, parasites, etc.) can be delivered in the form of liquids, aerosols or solids.
- **Chemical** agents can be delivered as airborne droplets, liquids, aerosols, or solids. They are categorized as classical chemical warfare agents (nerve, blister, blood and choking agents) and common chemicals used in and around the industry (e.g., pesticides, cleaners, antibiotics and heavy metals).
- **Physical** agents are materials that could cause adverse health effects if eaten (e.g. bone slivers, glass fragments and metal filings).

Defeat of the **forced** entry tactic relies not only on physical barriers, but also detection (e.g. broken seals) and interception by a responding force. The purpose of physical barriers is to delay an intruder long enough for a responding force to successfully apprehend the intruder or discourage his/her attempt at aggression.

The basic defeating strategy for **covert entry** or **insider compromise** tactics is to keep people from entering areas that they should not enter. This strategy relies on the use of increased awareness of who should or should not be in an area and where possible restricted entry or detection systems.

B. Security

"A security program is as good as its weakest link" RCMP

1. *General Security "Rules of Thumb"*

- Conduct regular security checks for signs of tampering with product or equipment, other unusual situations or areas that may be vulnerable to tampering. **Regularly review all initiated procedures to insure the level of security planned is functional (Record#4).**
- Assign responsibility for security to qualified individuals. Provide appropriate level of supervision to all employees, including cleaning and maintenance staff, contract workers, data entry and computer support staff, and especially new employees.
- Train all staff to be alert to any signs of tampering with product or equipment, other unusual situations, or areas that may be vulnerable to tampering.
- Provide encouragement and support to report any suspicious activity. Management may need to develop a system of rewards, and build specific tasks and responsibilities into job performance standards.
- Any suspicious findings must require immediate investigation of and the local law enforcement should be alerted if criminal activity is suspected.
- Evaluate every request for information about your operation. Never provide information over the phone.

2. *Tanker Requirements*

Many tankers will require retrofitting to ensure that seals function properly and vulnerable points of access be removed.

- Have ready-made signs available in the truck that clearly identify that the tanker contents are not fit for human consumption.
- Place signs on any outlet valves located on tankers at all access points.

Seals

- Only non-reusable seals that are approved and supplied by the BCMMB may be used.

Hatches

- All hatches must have two seal points approximately 180° apart

Pump Compartments

- Pump compartments must be sealed when unit is away from driver's control.

External Hoses

- External hoses must be capped and sealed when not in use.

Wash Line Inlets/Valves

- Wash line Inlets/Valves must be sealed.

En Route Tanker Security

- When the driver is preparing to leave on his/her collection route, he/she must check to verify that the numbers on the seals correspond to the numbers that were entered in the **Seal Log Sheet (Record #1).** If the numbers match, the driver writes his/her initials on the seal record.

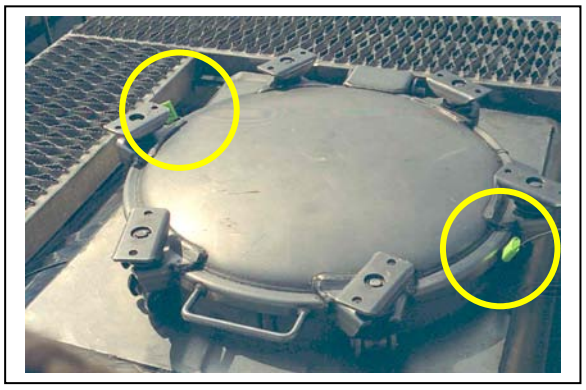
- When the tanker arrives at the first farm pick-up, the driver checks all seals to be certain that none are broken. The driver then breaks and removes the seals to the pump compartment and the inlet valve. The numbers on the broken seals are recorded and milk pick-up procedures begin.
- If at anytime the driver finds that a seal has been broken without his/her knowledge or that a seal is missing, he/she must immediately notify the supervisor. **Do not pick up any more milk until instructed.**
- Any time the tanker is not in visual contact or control of the driver, all milk contact openings on the tanker must be secured with a seal (e.g. out of sight, on the yard, etc.)
- At the last farm pick-up the driver attaches a numbered seal to the pump compartment, inlet/outlet valve(s), hatch, or any other milk contact point of access that has been opened. The seal numbers must then be recorded on the **Seal Log Sheet**.
- Once the tanker arrives at the receiving plant, authorized

receiving personnel compares the numbers on all the seals to the numbers in the **Seal Log Sheet** and sign to accept load.

- A milk tank truck transporting milk and milk products to a milk plant from another milk plant or transfer station must also remain sealed.
- Decision to seal or not:
  - If the tanker, after unloading at the plant is returning for reloading - all access points are re-sealed, and the numbers recorded on a new **Seal Log Sheet** (Record#1)
  - Tanker is travelling directly to wash station - seals may be absent after the tanker is unloaded if it is travelling directly to the wash station and won't be left unattended at any time. Drivers must always be in the control of the tanker – if at any time the driver is away from the tanker, then all access points must be resealed.
  - Resealing after washing and/or unloading is the responsibility of the driver.

Seals and Seal Log Sheet

The placement of seals on all access points to the milk contact surfaces reduces the risk of deliberate contamination of the raw milk during the various steps in the collection and delivery of raw milk to the processing plant. The ultimate goal is to have all openings to milk contact surfaces on the milk tankers sealed at all times, except when the tanker is being loaded, unloaded, sampled, washed, or is in the control of the driver.



- A **Seal Log Sheet** (Record#1) must be kept with the unit at all times. It will record the date, driver/receiver/washer who removed the seal(s), tanker numbers and seal numbers. Recording seal numbers will provide a chain of custody for each delivery of milk.
- Seals would be placed wherever access to milk contact surfaces can occur
  - manhole (2 places at 180 degrees to each other),
  - pump compartment
  - External Hoses
  - wash line inlets/valves.
- Seals are installed:
  - after washing,

- when not in attendance, visual contact or control of driver (e.g. tanker parked overnight, tanker in repair shop, etc.)
- after any access (e.g. to sample load, or in cold climates when the air vents freeze up and have to be cleaned up.)

- At the plant the receiver checks the seal before accepting milk and matches seal codes with Seal Log Sheet and if satisfied signs the seal record.
- Seals not in use must remain locked in the dispatch office or truck, or in the driver's possession**.**

Broken Seals

If a seal is broken, missing, or does not correspond with the Seal Log Sheet, or is damaged the following applies:

- If a seal is broken to complete a task (e.g. washing, sampling) the access points must be resealed after the task is done. The new seal number and the date/time it was installed must be recorded on the Seal Log Sheet.
- If a seal is broken without any known cause, notify supervisor. If the tanker is:
  - empty – tanker must be re-washed (as instructed by supervisor) before next milk pick-up, and investigate as requested.
  - full – milk is not to be unloaded, and the tanker must be identified. Driver awaits further instructions re unloading/disposal.
  - Suspected contaminated full or empty – wait for further instructions regarding any special disposal/washing requirements (see recall procedures in Incidence Response section). Details surrounding the incident must be written in the "corrective action" column of the Seal Log Sheet.
- It is the responsibility of the TMR to insure all broken seals are retained for verification.

3. *Communications*

- Communication within the tanker yard and the truck (cell phones, satellite tracking, radios, etc.) should be available to ensure that all key personnel can be reached, at all times.
- Develop an information/feedback system for all staff to report discrepancies, inefficiencies or improvement ideas. Report back any security messages to employees in various methods such as newsletters, bulletin boards, etc.

4. *Periods of Readjustment – Security Risks*

Rapid changes in procedure or events both within and external to the company can create breeches in security. Plan in advance how they may be handled to ensure gaps are filled before they happen. For example:

- Abrupt changes in routes, drivers, procedures, etc. (e.g. are new people trained, will the confusion cause relaxing of tasks, etc.)
- Terrorist activities tend to happen in groups. Security awareness should be heightened if new attacks begin anywhere.
- Increase security measures/awareness any time Canada begins military activity in foreign countries, or whenever employer-employee and/or farmer/hauler conflicts occur.
- Request that drivers watch for any suspicious activities in their vicinity. If drivers witness any suspicious activities, they should immediately report it to the designated supervisor trained for incidence response.

5. *Incidence Response*

Responding to a tampering, criminal or terrorist event swiftly and concisely will minimize the damage to both your operation and the milk industry. To be prepared for a crisis, the following points need to be considered in advance:

- Have a strategy pre-planned for the event.
- Have mock exercises every 6 months – level of staff involvement may vary from a simple paper exercise to an actual on-the-ground exercise with full staff involvement. The process should include an evaluation of how well and how fast the problem was detected.
- Identify in advance the critical decision-makers.
- Identify in advance, washing instructions for the suspected or determined contaminates.
- Identify management that employee's should alert about potential security problems (e.g. identify the recall team leader for every shift).
- Identify a 24-hour contact information listing of all company contacts and related companies, plants and local authorities. Repeat process for other provinces/regions that the milk is shipped.
- If a phone threat is received, have the following list accessible to all phone personnel and have them record or write notes on what they hear during and after the call. Consider having a checklist made that phone personnel have on hand.
  - Voice characteristics.
  - Background noise.
  - Name of person who answered the phone.
  - Time call was received.
  - What caller said?

- Exact threat that was made.
- What demands were made?
- If the caller indicated that they would call again.
- How long you spoke with the caller.
- How old did the caller sound?
- Gender of caller.
- Any accents noted.
- Caller's attitudes (calm, excited, intoxicated, rational, irrational, angry, and/or vulgar).
- Note if the call sounded as though it came from a car, phone booth, or building.
- Immediately after the call, dial *57 to mark the caller's call. Then, call the police and tell them that you marked the call by dialing *57. They in turn will be able to access from the telephone company the date and time the call was made and the phone number of the caller.
- Notify supervisor.

Example

Ineffective contact practices and preparedness caused one load to be destroyed because the time of discovering the problem and knowing what to do caused the tank temperature to exceed the required level.

Recall strategy

Should a seal be broken or a contamination identified:

- Identify a person on every shift to lead the recall procedure, but always have a back-up person for holidays, sick leave, etc.
- Provide for proper identification of any suspect tanker, and implement a protocol (markers, storage location, and disposal process) for withholding a tanker if tampering is suspected.
- Should the tanker get unloaded at a plant, the Canadian Food Inspection Agency (**CFIA**) has a 24-hour emergency product recall number (604-666-3350) where a 24 hour public food recall emergency announcement can be made.
- If criminal tampering or terrorism is suspected, the recall team leader should also notify local law enforcement.

Disposal Strategy

If a tanker that contains milk has been identified as unsafe, it must be disposed of using the following steps:

- Have ready-made signs available in all the trucks that clearly state the contents of the truck are not fit for human consumption.
- Place signs in holders, located on trucks at all access points.
- Do not intentionally release any of the contaminated milk or milk samples until all proper authorities have been notified.
- Keep all seal logs and any broken seals. Always maintain a copy of the seal log with you.
- Communicate details of the incident to all identified crisis/emergency personnel, particularly regarding the location and type of suspected hazard(s) involved.
- Do not leave the tanker or move the vehicle. If the vehicle/tanker must be left unattended, the tanker must be clearly marked. If the vehicle/tanker must be moved notify the crisis/emergency team of its new location.
- Do not attempt to identify any hazardous material by smell or touch. Reseal the tanker (if unsealed) and note the seal numbers.
- Keep all unauthorized persons away from the tanker.
- Transfer contents from the tanker only if instructed by the crisis/emergency personnel. Follow instructions from on where/how to wash the tanker and if it can re-enter back into regular use.
- The crisis personnel must receive approval from British Columbia Milk Marketing Board ("BCMMB") for a dumping site.

6. *Program Evaluation*

Evaluating the lessons learned from past tampering events, mock exercises and other related security issues can help improve existing programs. To effectively evaluate an operations program, the following should be in place:

- Annual review of strategies by conducting mock criminal, terrorist or tampering event and mock recall. Challenge computer and physical security system as well and revise accordingly.
- Perform routine and random security inspections of facility (including receiving, dispatch and storage areas and any related intrusion detection systems).
- Verify that security contractors are doing an adequate job.
- Consider using a third party or in-house security expert.

C. Sample Records

The following records must be kept in order to meet the requirements of the *Seal-Tite* Program:

1. Seal Log Sheet
2. Staff Training Records
3. Emergency Plan
4. Security Review Checklist
5. Standard Operating Procedure for Sealing Milk
6. Standard Operating Procedure for Suspected Contaminated Milk

You may use the following sample records or you may use your own. If you choose to provide your own, they must contain all the mandatory data items listed in the samples.

Record #1 - Seal Log Sheet

Tanker #_____

Seal #	Location[a]	√		Date	Plant	Time	Initials			Corrective Action
		Off	On		Code		Washer	Driver	Receiver	

a. Location: H1=Hatch seal #1; H2=Hatch seal #2; W=Washline (rear); P=pump compartment.

Others: _____

Record #2-Personnel Training Record: Sign–in Sheet

Date: _____	**Topic Discussed:** _____ _____
Name:	Signature:

Record #3 - Emergency Plan

Failed BMP	*Specific Incidence*	*Action To Be Taken*	*Contact Person*		
			Name	**Phone**	**Cell Phone**
Broken seal (1 or more)	1. Milk tanker empty – seal missing or damaged				
	2. Milk tanker full – seal missing or damaged				
Water use in wash station contaminated	Water test result high bacteria				

Failed BMP	*Specific Incidence*	*Action To Be Taken*	*Contact Person*		
			Name	**Phone**	**Cell Phone**
Milk tanker swabbing shows high bacteria	Location: _____				

Record #4: Security Review Check List

A thorough review of your company's security strategies should consider each of the following:

- ❑ people
- ❑ inputs (paper goods, chemicals, equipment, building materials, etc.)
- ❑ facilities and processes
- ❑ crisis management procedures
- ❑ evaluation
- ❑ training process

Keep in mind the three main areas of hazard introduction when reviewing each strategy area: 1. Cross-contamination potential; 2. Incomplete procedure/steps that will result in uncontrolled hazard introduction; and 3. Accidental or deliberate introduction of contaminates.

Practice	Verified √		Problem / Corrective Action
	Yes	No	
Facilities			
Is there sufficient awareness in place with regard to security to prevent unauthorized access by visitors within the boundaries of the facility?			

Practice	Verified √		Problem / Corrective Action
	Yes	No	
People			
Have standard operating procedures been developed and implemented for drivers when they leave tankers unattended for meals, gas, breakdowns, etc.?			
Are there predetermined SOPs in place and known by drivers when faced with suspicious circumstances?			
Are programs in place for instruction/training of staff to understand procedures and be aware of what constitutes suspicious activity?			
Do employees know how to reporting suspicious activity to management? Is there a recall plan in place?			
Are employees aware that security details are kept confidential?			
Does the new employee orientation program include broken seal procedures and procedures for dealing with various suspicious situations? Does the orientation program include instructions for employees on what to do if they suspect wrongdoing or product tampering?			

Practice	Verified √		Problem / Corrective Action
	Yes	No	
Inputs			
Does the wash station have a program in place to identify all sources of water used in the facility? Are security measures associated with each source of water (testing potable water) If a municipal water supply is used? Are there predetermined procedures for prompting two-way communications with responsible municipal officials in the event of any abnormalities?			
Are cleaning and sanitizing chemicals, lubricants, paints, pesticides and other non-food chemicals stored away from wash stations, under controlled access and with documented inventory control?			
Trucks/Tankers			
Is there a SOP on how drivers keep tankers sealed?			
Is there a capability for verification of driver location and load at any time?			

Practice	Verified √		Problem / Corrective Action
	Yes	No	
Are seals and logs in a secure area to prevent theft and misuse?			
Crisis Management			
Are specific SOPs outlined for investigating any suspected security situation that might be identified?			
Is there a detailed written plan in place to identify who does what, where, how and when? Are there key contact people identified and known to staff, and are de-contamination procedures in place? Are crisis procedures always known by someone on every shift?			
Are mock crises ever done to test specific procedures and employee awareness?			

Record #5 - Standard Operating Procedure for Sealing Milk Tanker Access Points

In order to ensure that **milk is secure from tampering**, describe step-by-step the various actions and access points that should be taken to seal a tanker.

Step 1_____

_____

Step 2_____

_____

Step 3_____

_____

Step 4_____

_____

Step 5_____

_____

Step 6_____

_____

Record #6 - Standard Operating Procedure for Suspected Contaminated Milk

In order to ensure that **any contaminated milk is <u>not</u> accidentally added to the system**, describe step-by-step the various steps that should be taken:

Step 1_____

_____

Step 2_____

_____

Step 3_____

_____

Step 4_____

_____

Step 5_____

_____

Step 6_____

_____