Canadian Grain Commission   Commission canadienne des grains

FOOD DEFENCE SELF-ASSESSMENT CHECKLIST
GRAIN HANDLING FACILITIES

Copy No. Uncontrolled

Canadian Grain Commission
Process Verification and Accreditation Office
Industry Services
900-303 Main Street
Winnipeg, Manitoba
Canada R3C 3G8

April 1, 2017

Revision 1

Table of Contents

Food Defence Self-Assessment Checklist
Grain Handling Facilities

The first part of developing a Food Defence good operating practice is to perform a self-assessment of your current security and food defence practices. This self-assessment will help you determine which policies and practices you may already have in place to prevent intentional tampering, and as well, will serve as a guide to helping you implementing food defence good operating practices.

This checklist is not an exhaustive list but is meant to be a guidance tool for assessing your facility's compliance to PPR-015 Food Defence. You may encounter critical areas or assets not covered in this checklist that are specific to your facility that may be at risk to tampering or intentional contamination. Likewise, you may also find that your facility has dealt with potential food defence risks in ways that are not suggested by this checklist. The best way to use this checklist is to compare the recommended practices to your facility's current practices, adding security measures where deficiencies are found and omitting recommendations that are not applicable to your facility or where other measures adequately cover the risk.

Using this Checklist

Each section focuses on an asset or process that may be at risk and lists a series of options that may be used to increase the security of that asset or process. Security options for each section may include, but are not limited to, one or a combination of any number of the options given.

If "no" is selected for a security option, it is highly recommended that your facility consider implementing policies, procedures and infrastructure to enhance the security for that particular asset or process. There may be options that are not feasible for your facility or may be deemed excessive for your operation (e.g. installing fences around your facility, video surveillance cameras). If this occurs, then the following questions should be considered:

1. What is the risk to the asset or process if this security option is not implemented?
2. Are there other security measures implemented or that can be implemented that would mitigate any security breach of that asset or process?

Determining Risk

Determining whether an asset or process is at risk involves thinking about these assets and processes from the perspective of an attacker wanting to do harm. You want to identify the most attractive targets for attack and what points in your facility's infrastructure or operations are most vulnerable. Once you have determined which assets or processes are most at risk, you can then focus resources on reducing the likelihood of security breaches within your facility.

Using a risk assessment model, such as the CFIA model shown in Figure 1, may help to assess the significance of a food defence breach. This may help you to decide where resources are best allocated for your facility's food defence plan.

If you answer "no" to any of the questions in the checklist, you should consider:

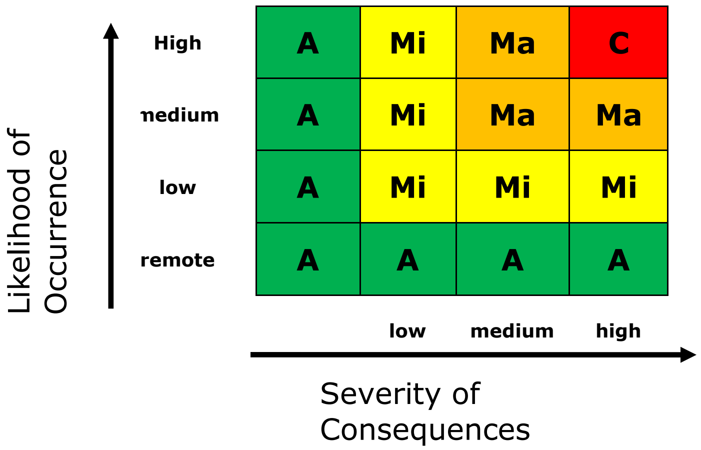
- How likely is it that an attack could occur without this measure in place?
- How severe are the consequences if there was an attack?

The likelihood of occurrence as depicted on the vertical axis (Figure 1) refers to the chance that an attack may occur. The likelihood of a breach in security increases as control over assets and processes decreases.

The severity of the consequences as depicted on the horizontal axis (Figure 1) refers to the impact that intentional taint or tampering will have on human health. The severity of consequences is broken down into one of 3 categories:

Low – no medical attention required
Medium – medical attention required, but full recovery of consumer expected
High – medical attention required, no chance of recovery of the consumer

To determine the risk of tampering or intentional taint, combine the results of the likelihood of occurrence with the severity of the consequences. The outcomes vary based on the likelihood that tampering or intentional taint will occur and the severity of the consequences.



		low	medium	high
High	A	Mi	Ma	C
nedium	A	Mi	Ma	Ma
low	A	Mi	Mi	Mi
remote	A	A	A	A

There are four levels of risk in this model:

Acceptable (A) – a very small possibility of risk
Minor (Mi) – a low level of risk
Major (Ma) – a moderate level of risk
Critical (C) – a high level of risk

Depending on the outcome of your risk assessment, you may need to evaluate whether or not another security measure will mitigate this risk or if additional security measures are required. It is impossible to eliminate all risk, but you must be able to ensure that risk is reduced to an acceptable level.

When completing this checklist, conduct the risk analysis for each section to which you answered “no” and then document your justification for your risk mitigation action. It may be as simple as having another security measure in place that will protect the process or asset. If you find that a process or asset is not adequately addressed, other security measures may need to be implemented.

Physical Security of the Facility

Required outcome: physical barriers and deterrents are installed to deter intruders and prevent access to the facility

Assessment: What type of physical security measures does your facility have to prevent unauthorized access to the critical areas or assets of your operation?

	Yes	No	N/A
Unattended entry points (doors, windows, ventilation system access) to the facility are secured with locks, seals or sensors			
Security lighting in high risk or dimly lit areas			
Motion activated lighting in high risk areas			
Motion detection devices and alarms that are monitored by an off-site security company or contractor			
Video surveillance equipment in high risk areas			
Surveillance patrols by a contracted security firm			
Perimeter fencing around the facility with locked gates			

Risk analysis and mitigation:

Access to the Facility

Required outcome: access to assets or processes that are at risk for tampering or taint is restricted for unauthorized persons

Assessment: What type of operational security measures does your facility have to prevent unauthorized access to the critical areas or assets of your operation?

	Yes	No	N/A
Designating sensitive or high risk areas of the facility as restricted areas (e.g. chemical storage, utility system access, areas used to store sensitive information) and controlling access to these areas			
Maintaining employee shift schedules to ensure that supervisors know which employees to expect on-site			
Limiting employee access to critical areas or assets of a facility based on employee job function			
Designating specific areas for parking, keeping staff parking separate from visitor parking			
Requiring all visitors, contractors and vendors to sign in with a designated company representative upon arrival			
Requiring all visitors, vendors and contractors to be accompanied while on the premises			

Risk analysis and mitigation:

Assessment: How is the grain handling process flow secured in your facility?

	Yes	No	N/A
Preoperational assessment of the premises and equipment is conducted to inspect for signs of tampering, vandalism or breach of security			
Exterior ladders are locked/access is restricted			
Receiving pit is covered and secured when not in use (e.g. after hours)			
Grain discharge spouts are secured when not in use			
Storage bins and containers are secured when not in use			
Doors to maintenance and tool sheds and chemical storage areas are secured			
Access to the facility’s control room is restricted			
Access to the facility’s power supply (e.g. electrical panels, generators) is restricted			
Computer-generated information is safeguarded; information is password-protected; anti-virus software is installed and updated; and saved data is backed up and stored off-site			
Inventory records of all grain and non-grain inputs are kept current			
Physical records (documents, scale tickets, bills of lading etc.) are stored in a secured, locked area			
Restrict access to company keys and/or limit access to authorized personnel only			

Risk analysis and mitigation:

Personnel Procedures

Required outcome: procedures are in place to ensure that employees of the facility are unlikely to pose a food defence risk to the facility or its operations

Assessment: Does your facility have food defence personnel procedures in place?

	Yes	No	N/A
Resumés are requested from applicants; qualifications are screened; and multiple references are contacted			
Short-term and seasonal employees are restricted from accessing critical assets or areas			
Work assignment schedules are developed and maintained			
Employees are trained in food defence and security policies and procedures, including whom to contact in case of emergency, which areas of the operation are high risk and where the shut-off points are for utilities. Training is conducted on a regular basis for new employees and as a refresher for existing employees			
Employees are trained to report suspicious activities or behaviours, misplaced equipment or suspicious materials or devices			
Supervisors and management are trained to be alert for atypical illness or health conditions among employees			
When employees are terminated or resign, all employee identification, facility keys, access cards, cell phones and other company electronic devices are returned			
When employees are terminated or resign, all access to information (e.g. computer log-in and email accounts) is suspended			
When employees are terminated or resign, company records are updated to reflect this change in authorization and customer contacts are notified in the change in authorization			
Contractors performing work on site are briefed on the facility's security rules and what areas of the plant they are allowed to access			
Truck drivers delivering grain and non-grain inputs are restricted to receiving areas only			
The entry of employees into the facility during non-working hours is restricted to authorized personnel only			
Employees and contractors are prohibited from bringing personal items not required for job performance into the grain handling area			

Risk analysis and mitigation:

Receiving and Shipping Procedures

Required outcome: inbound and outbound grain and non-grain inputs are not potential targets for taint or intentional contamination

Assessment: what procedures does your facility have in place to ensure the security of the receiving and shipping operations?

	Yes	No	N/A
The company has a supplier approval program for purchasing non-grain inputs			
The company has a producer approval program in place for purchasing grain			
Grain is inspected upon receipt for evidence of taint or tampering			
Non-grain inputs are inspected upon receipt for evidence of taint or tampering			
The receiving area, including the pit, is inspected as part of the facility's start-up procedures			
Transport affidavits are required before incoming grain is received at the elevator			
Transport conveyances (railcars, containers, trucks) are inspected before grain is loaded for shipping			
Outgoing shipments are sealed with tamper-evident seals and the seal number is documented on the outgoing shipping documents			
Access to receiving areas and loading docks are monitored			
Unfit and contaminated goods are segregated in a way that minimizes the likelihood of compromising other goods			
Security measures and procedures are in place at all off-site and public warehousing locations			

Risk analysis and mitigation: