IFS HPC version 2
Product Defense guideline

Background

Due to recent events, security awareness has become an important issue for multiple industries worldwide. From the food industry, where the Food Defense programs are well known to guidance from the FDA on cosmetics security preventive measures.
This show us how the idea of tampering or malicious actions has become a relevant topic for many industries.
It is important to understand that for raising awareness on Product Defense should be taken into consideration factors like the product itself, site security and human factor, among other requirements.
Within a company, Product Defense flow starts from the Senior Management commitment to the employees; it goes from the top to the bottom.

This Product Defense chapter in the IFS HPC V2 Standard was developed in order to start building consciousness between the household and personal care manufacturing industries about possible risk of tampering or other malicious, criminal, or terrorist actions around the product with severe consequences.

This guide will provide the IFS HPC certified suppliers, a better knowledge about the intent of the Product Defense requirements, and an understanding of implementation practices and considerations.

Moreover, the recommendations in this guideline should not be regarded as minimum standards. Nor should the examples provided be considered an inclusive list of all potential approaches to achieving the goal of the preventive measure.

The IFS HPC Product Defense chapter is primarily aimed at companies exporting to the United States of America, or companies which export and/or produce in countries where this topic is also legally relevant. The chapter is also applicable in the event of specific customer requirement.

For the other companies, the chapter may be assessed as not applicable by the auditor (N/A).

General structure of the program

Product Defense programs may include the following criteria which may be modified depending upon the country, organization and regulatory requirements.

- Clear roles and responsibilities, management commitment and employee awareness.
- Hazard analysis and assessment of the associated risk of the product, facility, facility surroundings to identify vulnerabilities.
- Identification of vulnerabilities and determination of control measures.
- Internal audits of the entire Product Defense program.

- To have a security management strategy to prepare for and respond to tampering or other malicious, criminal, or terrorists actions, both threats and actual events, including identifying, segregating and securing affected product.
- Continual improvement of the system.

Guideline for chapter 6 of IFS HPC V2: Product Defense

6.1 Senior Management Responsibility

A Product Defense team or a single person, with accountability to the facility management team shall be established with defined roles and responsibilities. Defense is the responsibility of the Senior Management and is therefore a "management issue".
The team shall have access to the management and preferably with experience in the area of security. Competence can be gained through training and/or relevant experience in this area.

6.1.1 The company shall have a documented product defense procedure in place to address product defense risk from products and establish, implement and maintain a system to reduce or eliminate the identified risk.

The auditor shall perform an assessment of the Product Defense program regarding its implementation and the relevant associated documents.
IFS does not define how this procedure shall look like. The company is free to develop its own tools/programs.

Regardless of how the applied program looks like, all relevant security aspects of the location shall be taken into account. Records are evidences of effective implementation and provide information about the extent to which the Product Defense program is confirmed.

6.1.2 A product defense assessment shall be conducted annually or upon changes that affect product integrity.

The result of the product defense hazard analysis and assessment of associated risk should be an identification of conditions that pose a risk of intentional acts to the process, materials, and product resulting in adulteration.
Reviewing and verifying, at least annually or upon changes, the effectiveness of the security management program (for example, using knowledgeable in-house or third party staff to conduct tampering or other malicious, criminal, or terrorist action exercises and mock recalls and to challenge computer security systems).
Revising the program accordingly, and keeping this information confidential.

In order to identify vulnerabilities the Product Defense team should consider the following criteria (by no means exhaustive):

- **Exterior**
  - Are doors, windows and roof areas kept secure?
  - Is a perimeter fence or wall necessary? If a perimeter fence or wall exists, is it in a good condition?
  - Is there adequate interior and exterior lighting, including emergency lighting?
  - Is there controlled access of people and vehicles?
  - Are there back-up sources of critical utilities, such as electrical, water, computer data and refrigeration systems available, in case of emergency?
  - Are parking areas controlled and monitored?
  - Are ventilation systems adequately protected?
  - Are bulk receiving and storage areas secured?

- **Interior**
  - Are surveillance methods utilized, such as cameras, staff supervision, or security services?
  - Are there systems that effectively alert employees in case of security breach?
  - Is access controlled?
  - Are hazardous materials or controlled substances managed?
  - Is access of staff limited to appropriate work location, job function and working hours?

- **Receiving and shipping**
  - Are transportation vessels sealed/ locked?
  - Are drivers providing appropriate credentials?
  - Are deliveries and shipments scheduled?
  - Are transportation vendors part of the vendor approval program?
  - Are suspect products/ raw materials rejected?
  - Are any unexplained or delayed deliveries investigated?

- **Raw Materials**
  - Are water, ice and steam sources secure and monitored?
  - Are all raw materials secured and monitored when not in use?
  - Are there means to verify integrity and chain of custody?
  - Are packaging materials and product labels controlled?

- **Personnel**
  - Are personal background checks necessary or performed, if allowed by law?
  - Is the potential for retaliatory actions by terminated employees assessed?
  - Are the reasons for an employee's departure reviewed?

- Are personnel supervised?
- Are employees trained in Product Defense awareness and identifying / reporting unusual or suspicious behavior?
- Are lockers inspected?
- Are cameras allowed?
- Are personal items restricted in processing areas?
- Is there a policy written to address legal or illegal weapons and drugs?

- **Access to computer systems**
  - Is there any restriction access to computer process control systems and critical data? Only those with appropriate authorization should have access to critical data access.
  - Is there anybody responsible for eliminating computer access when an employee is no longer associated with the company?

Once the company identifies risks and vulnerabilities, appropriate control measures should be developed and implemented based on the elimination, mitigation, and maintenance of risk to an acceptable level.

6.1.3 Responsibilities for product defense shall be clearly defined. Those responsible shall be key staff or shall have access to the senior management team.

A Product Defense team (it could be a person or a team) with accountability to the facility management team, shall be established with defined roles and responsibilities reviewed on a regular basis.
In case of a team, this team should include cross-functional employees from all levels within the organization. They should possess the knowledge and expertise to identify program requirements and propose the best course of action. A team leader should be identified whom is responsible for the coordination, development, implementation, maintenance and improvement of the system.

If applicable (if Product Defense matters are applicable in the production and destination countries of products), there should be a designated contact and process for communicating with the local and national authorities.
Product Defense training should be provided to employees appropriate to their duties.
Senior management review should include the Product Defense program (if applicable).

Example of questions to be asked by the auditor:

1) Who has the accountability for the Product Defense program?
2) What are the competence and qualifications demonstrated for the person(s) responsible for the Program Defense program?
3) What is the position of the person(s) responsible for the Product Defense program with respect to the Senior Management team?
4) How does Senior Management support the person(s) responsible for the Product Defense program?
5) Where are the responsibilities clearly defined?

6) Was this communicated to the members of the company? How?

6.1.4 Senior management shall have an internal communication system to inform and update staff about relevant security issues.

Example of questions to be asked by the auditor:
How this information is communicated to all personnel? By which means? E.g. bulletins, internal notes, etc.
All employees are aware of this communication? Even temporary workers?
Have an internal communication system to inform and update staff about relevant security issues.

6.2 Site security

The key point is to prevent unauthorized access to product, ingredients and services that could adversely affect the content of safety of the products.

Easily accessible raw materials, intermediate and finished products or even chemicals (cleaning agents, acids, lye, flammable liquids, toxic chemicals, etc.) could be stored in specific areas as far away from manufacturing areas as practical.
Classic points to be considered are the outside storage of materials, unlocked doors or other installations that limit access. The overall goal of Product Defense is site security. Fences can help in this task, but are not mandatory if security can be achieved through other measures. For instance, visual surveillance or security personnel could be just as effective. Uncontrolled access in storage and production areas is in no case acceptable.

If critical areas were identified, they can be monitored with specific construction measures, such as security doors or access with chip cards. Specific attention should be paid to raw materials, equipment and materials that are stored outside, which must be protected from unauthorized access in case of possible product hazard through manipulation.
Controls for incoming and outgoing goods such as seals and labels can provide additional security.

Physical barriers, procedures and systems should be established that prevent unauthorized access to areas external to the plant, internal to the plant, to laboratories handling chemicals and reagents, to waste disposal areas where potentially hazardous materials are disposed of and to service areas such as water, gas, electric, refrigeration systems, etc. Such barriers and procedures should, taken in their entirety, provide adequate protection of product and systems used to manufacture and store it. Measures established should be appropriate to effectively manage the associated risk. The key to establishing such measures is to assure they are effective and appropriate. There are many ways to manage risk and many types of situations that create risk of unauthorized access. Examples of methods used to control unauthorized access can include fencing, guards, security alarms, electronic pass keys, locked doors, windows that do not open, cameras. In general, such measures should protect product that is stored both inside the plant and external to the plant. Storage bins/silos would be included.

Computer systems are often fire walled and password protected. Procedures such as sign in procedures, keeping doors locked, etc. can supplement or substitute for physical barriers.

Access points shall be controlled:
Through a combination of physical barriers, procedures and systems that work together to prevent unauthorized access.
Access points should be controlled. Not all entries are access points. If a door is locked at all times, it is not an access point. If windows are continuously locked, they are not necessarily an access point. Control may be maintained through basic procedures and / or high tech systems that could be equally effective.
Generally this clause applies to access from the outside to the inside of the facility but also applies to external storage vessel and vehicles access, as well as access from one critical area in a plant to another.

6.2.1 Based on the product defense procedure and legal requirements, the senior management should define and communicate the areas in which authorized personnel are allowed to access.

Example of questions to be asked by the auditor (this is also connected with requirement 4.5.1.2)
1) Based on the hazard analysis and assessment of associated risk, what areas have been identified as critical?
2) What control measures are in place in order to control the entrance to those areas?
3) How does the company maintain control over who enters to the premises and critical areas?
4) What are the access controls applicable to the following people?
- Temporary employees
- Contractors
- Visitors
- Employees
- Carrier drivers

Moreover, it is important that the Senior Management has identified which personnel have access to certain areas and which don´t.

6.3 Visitor and Personnel Security

In order to protect against misuse, the company shall limit and control access to the premises, especially sensitive areas.
In addition to registering visitors and service providers on the premises, adequate briefing and supervision should take place. This also includes equipment and materials brought from outside. For example, chemicals, knives with retractable blades, lubricants or even workers themselves must all be considered.

Employees shall participate at regular product defense training. Concretely, this means conducting documented training on main product defense aspects at least once a year. Main goal is to increase sensitivity of employees to product defense aspects. Employee surveys is a way to assess if employee are sensitive or still unfamiliar to the subject.
The team responsible for product defense should attend at more intensive training (if available).

A difficult and sensitive subject is the employee background check, because this is differing to countries and customs. For example, in the USA, reviewing criminal records and other documents by specialized firms and drug tests are common, whereas such measures are legally very limited or sometimes even prohibited in other countries.
Finally, another concern is that a company is able to ensure that new employees are trustworthy, reliable and pose no security risk. If background checks are not possible or unwanted, other references can be, for example, job references, telephone interviews of former employers, recommendations, or a police clearance certificate depending on the position.

6.3.1 Visitor policy shall contain requirements relating to product defense.

Example of questions to be asked by the auditor:
1) Do visitor / contractor access policies include controls to avoid that no members of the company are able to move freely without escorts inside the premises?
2) Are visitors and contractors informed of the product defense rules and their scope while inside company premises?
3) Does the company have defined means to ensure that contractors who will spend a long time inside the plants are properly identified, supervised and escorted inside critical areas?
4) Are there controls to ensure that truck drivers who load or unload products/materials are restricted to defined areas inside and outside the building and company premises? Are there means to watch the movements of non-employees once they enter to the company´s premises? (E.g. cameras or guards at defined areas? other procedures?).
5) If contractors and visitors are provided with access keys, are those keys programmed to limit the access to specified and selected areas?
6) If escorts are required to guide visitors and contractors at all times, are there arrangements to have defined guides at all shifts?
7) Are security/guards aware of how to deal in cases where there are no escorts available at any particular moment?

6.3.2 Employee hiring and employment termination practices shall consider security aspects as permitted by law.

Example of questions to be asked by the auditor:
1) What controls are implemented at the time of hire/termination of an employee or creation/termination of a service by a contractor?

2) Are access controls updated at the time of termination of an employee or when the work is finished on the part of a contractor?
3) Is the company´s computer access still available for an employee when is no longer associated with the company?

6.3.3 The company shall incorporate product security awareness, including information on how to prevent, detect and respond to tampering or other malicious, criminal, or terrorist actions or threats, into training programs for staff, including temporary, contract, and volunteer staff.
The training shall regularly take place and shall be documented.

The aim is to promote product security awareness to encourage all staff to be alert to any signs of tampering or other malicious, criminal, or terrorist actions, or areas that may be vulnerable to such actions, and reporting any findings to identified management (for example, providing training, instituting a system of rewards, building security into job performance standards).

Example of questions to be asked by the auditor:
1) Does the annual training program include Product Defense?
2) How is product defense and associated controls explained to new employees?
3) Are there records that demonstrate that employees received Product Defense training?
4) Is training updated according to changes in the Product Defense program?
5) How are employees informed of major changes in the Product Defense program?
6) Does the system evaluate training effectiveness?
7) Does training include controls of knowledge acquired from the last version of the Product Defense training?

6.4 Documentation requested by legislation
Regulatory requirements dictate whether or not registrations or on-site inspections are necessary. If they are necessary, then evidences should be available for review that indicate the appropriate regulations have been complied with.

The appropriate regulatory documentation whether local or national should be compiled and stored in general as the other documents required in the IFS HPC Standard.
This requirement is not applicable (N/A) if no legislation exists in the country where the audit is done and where the products are sold.

6.4.1 If legislation makes registration or on-site inspections necessary, these shall be carried out and evidence shall be provided.

Example of questions to be asked by the auditor:
1) What are the legal / customer product defense requirements applicable to the company?
2) Based on legal requirements in the country where the plant is located or by the country where the product is used, is it required to apply for formal registration?

3) If registration is required, who has this information? Could the company demonstrate compliance?
4) Is there any requirement for periodic inspection? If so, then:
    a) Who performs it?
    b) Against what Standard?
    c) When was the last inspection?
    d) What was the result of the inspection?
    e) Is it required to provide evidence that deviations have been solved? (Corrective Actions)
    f) What are the implications if a major breach is identified?

6.4.2 A documented procedure shall be in place for managing external inspections and regulatory visits (if applicable). Relevant personnel shall be trained to execute the procedure.

Example of questions to be asked by the auditor:
1) Is there a documented procedure that defines the criteria to follow in case an external organization requires access to the company's premises?
2) Are there clearly defined levels of authority to provide access to external organizations at all times?
3) Does the procedure define the means to proceed if or when a regulatory body requests access to the premises?
4) Are relevant functions aware of their responsibilities under such conditions?
5) Are levels of authority defined with respect to the kind of information that is allowed to be provided?
6) Are there means to ensure a complete record of activities done and details of the visit?