1. **SCOPE**
2. This procedure applies to all personnel working at Tijule.
3. **PURPOSE**
4. This Food Defense/Food Fraud/food fraud plan represents Tijule’s steps to minimize the risk of tampering for economic gain or other malicious, criminal, or terrorist actions against its products and within its processing controls. Our threat/vulnerability analysis is in compliance with Food and Drug Administration’s requirements (See [Food Defense/Food Fraud Plan Builder](file:///C:\Users\royne\AppData\Roaming\Microsoft\Windows\Start%20Menu\Programs\FDA))
5. Food Fraud/Food Defense is the prevention of **intentional** contamination of food. Food Safety is the prevention of **unintentional** contamination of food.
6. **PROCEDURE**

**Responsibility**

Members of the Food Defense/Food Fraud Team: Managing Director, Factory Manager, Food Safety Team Leader, Food Safety Coordinator, Sales and Marketing Rep., Security personnel will be called upon to aid team where necessary.

1. **Managing Director**
2. This Food Defense/Food Fraud Plan is divided into (6) sections that relate to individual Tijule functions;
   * 1. Management
     2. Employees
     3. Public
     4. Facility
     5. Operations
     6. Emergency “Point of Contact” List.
3. Preparing for the possibility of tampering or other malicious, criminal, or terrorist actions
4. Assign responsibility for security to knowledgeable individual(s).
5. Plan for emergency evacuation, including preventing security breaches during evacuation.
6. Make employees aware of whom in management they should alert about potential security problems (24-hour contacts).
7. Promote Food Defense/Food Fraud awareness to encourage all employees 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.
8. Have an internal communication system to inform and update staff about relevant security issues.
9. Ensure all incoming mails to be logged (sender and recipient) by secretary and recipients sign on receival. Only company related mails are to be received. No personnel mails will be allowed.
   1. **Supervision**
      1. Provide an appropriate level of supervision where necessary to all employees, including cleaning and maintenance employees and new employees.
      2. Conduct routine security checks of the premises.
   2. **Investigation of suspicious activity**
      1. Investigate threats or information about signs of tampering or other malicious, criminal, or terrorist actions.
      2. Alert appropriate law enforcement and appropriate regulatory bodies about any threats of or suspected tampering or other malicious, criminal, or terrorist actions.
      3. Products that have been contaminated or suspected of being contaminated are held in the non- conforming product area which is locked and access restricted. For disposal treat as non-conforming products (reference [Control of Non Conforming Products](file:///\\Dc2\j\FoodSafety\FSSC%2022000%20Management%20System\PROCEDURES\ManagementSystemProcedures\ControlOfNonconformingProducts\Control%20of%20Non-Conforming%20%20Product.docx) Procedure)
      4. Review customer complaints.
   3. **Evaluation program**
      1. Evaluate the lessons learned from past tampering or other malicious, criminal, or terrorist actions and threats.
      2. Review and verify, after each actual or potential failure or at least annually, the effectiveness of the security management program (Infiltration test). The following should be considered
10. Presence of security personnel on entering premises
11. Logging in and ID issue protocol
12. Level of freedom of movement once on premises
13. Ease of access to Receival, processing and warehousing areas
14. Did any employee stop and /or question you?
    * 1. Perform random Food Defense/Food Fraud inspections of all appropriate areas of the facility using knowledgeable in-house or third party personnel, and keeping this information confidential
    1. **Employees**

Examine the background of all employees.

* + - 1. Know who is and who should be on premises, and where they should be located.
      2. Keep information updated
    1. **Identification**
       1. Collect keys or identification badge when an employee member is no longer associated with the establishment.
    2. **Restricted access**
       1. Identify employees that require unlimited access to all areas of the facility
       2. Reassess levels of access for all employees periodically
       3. Limiting access so employees enter only those areas necessary for their job functions and only during appropriate work hours
       4. Employees entering storage areas (Spice, Packaging, Cold room) are required to sign Access Log .
       5. Shirt colors differentiate employees having limited or unlimited access to areas in the facility and to certain task. Employees in white shirts have unlimited access while employees in yellow are restricted to production and warehousing areas, purple shirts area restricted to cassava area, red shirts are assigned to sanitation personnel and grey for production trainees
    3. **Personal items**
       1. Restrict the type of personal items allowed in establishment
       2. Allow in the establishment only those personal use medicines that are necessary for the health of employees and ensure that these personal use medicines are properly labeled and stored away from production & warehouse storage areas.
       3. Prevent employees from bringing personal items into production or warehouse storage areas. Personal camera is not allowed.
  1. **(Public)**
     1. Visitors (Contractors, Supplier Representatives, Delivery Drivers, Customers, Couriers, Pest Control Representatives, Third-Party Auditors, Regulators, Reporters, Tours)
     2. Visitors, as described above, are logged in at security post and given an identification badge which must be worn visibly.
     3. Restrict entry to the facility.
     4. Ensure that there is a valid reason for the visit before providing access to the facility - beware of unsolicited visitors
     5. Verify the identity of unknown visitors
     6. Restricted access to food processing area and accompanied by company representative.
     7. Must complete non disclosure form prior to entering facility.
  2. **Facility**
     1. Physical security
        1. Protect perimeter access with fencing or other security deterrents.
        2. Secure doors.
        3. Monitor the security of the premises using appropriate methods.
        4. Provide adequate interior and exterior lighting, including emergency lighting, where appropriate, to facilitate detection of suspicious or unusual activities
     2. Scheduled Security Audits
        1. Audits to validate security shall be conducted on a quarterly basis.
  3. **Operations**
     1. Incoming materials and contract operations:
        1. Allow only Approved suppliers on the compound.
        2. Take reasonable steps to ensure that suppliers practice appropriate food security measures.
        3. Establish delivery schedules except for ackee, not accepting unexplained, unscheduled deliveries or drivers, and investigating delayed or missed shipments.
        4. Reconcile the product and amount received with the product and amount ordered and the product and amount listed on the invoice and shipping documents, taking into account any sampling performed prior to receipt
        5. Investigate all shipping documents with suspicious alterations
        6. Inspect incoming materials.
        7. Reject any suspected in-coming raw material
        8. Alert appropriate law enforcement and regulatory authorities about evidence of tampering, counterfeiting or other malicious, criminal, or terrorist action.
     2. Storage
        1. Keep track of incoming materials and materials in use, including ingredients, packaging and labels. Store product labels in a secure location and destroy outdated or discarded product labels
     3. Security of water and utilities
        1. Stay attentive for media alerts about public water provider problems, when applicable.
        2. Identify alternate sources of potable water for use during emergency situations where normal water systems have been compromised.
     4. Finished products
        1. Request locked and/or sealed vehicles/containers/and providing the seal number to the consignee.
        2. Request that the transporter have the capability to verify the location of the load at any time.
        3. Keep track of finished products.
        4. Investigate missing or extra stock or other irregularities outside a normal range of variation and alerting appropriate law enforcement and regulatory authorities about unresolved problems, when appropriate.
        5. Advise consignee to be on the lookout for counterfeit products and to alert management if any problems are detected.
     5. Access to computer systems
        1. Review the adequacy of virus protection systems and procedures for backing up critical computer based data systems
        2. Validate the computer security system

1. **RECORDS**

Visitor Log

[..\..\..\FORMS\PRP FORMSSS\Visitors Log in Sheet](file:///\\Dc2\j\FoodSafety\FSSC%2022000%20Management%20System\FORMS\PRP%20FORMSSS\Visitors%20Log%20in%20Sheet)

Customer Log in sheet

[T:\FSSC 22000 Management System\FORMS\Customers log.docx](file:///T:\FSSC%2022000%20Management%20System\FORMS\Customers%20log.docx)

Task Workers Log in Sheet

[T:\FSSC 22000 Management System\FORMS\Task workers register.docx](file:///T:\FSSC%2022000%20Management%20System\FORMS\Task%20workers%20register.docx)

Emergency contact list

[..\..\..\Emergency Contacts\Emergency Contacts.docx](file:///\\Dc2\j\FoodSafety\FSSC%2022000%20Management%20System\Emergency%20Contacts\Emergency%20Contacts.docx)

Visitor ,Vendor and Contractor Badges

[..\..\..\PreRequisitePrograms\Food Defence](file:///\\Dc2\j\FoodSafety\FSSC%2022000%20Management%20System\PreRequisitePrograms\Food%20Defence)

1. **REFERENCES**

Non-Disclosure Agreement

[..\..\..\FORMS\MS Forms\Non-Disclosure Agreement\Non-Disclosure Agreement.docx](file:///\\Dc2\j\FoodSafety\FSSC%2022000%20Management%20System\FORMS\MS%20Forms\Non-Disclosure%20Agreement\Non-Disclosure%20Agreement.docx)

Background Check

[..\..\..\FORMS\Background check form](file:///\\Dc2\j\FoodSafety\FSSC%2022000%20Management%20System\FORMS\Background%20check%20form)

Non-Conforming Product

[..\..\ManagementSystemProcedures\ControlOfNonconformingProducts](file:///\\Dc2\j\FoodSafety\FSSC%2022000%20Management%20System\PROCEDURES\ManagementSystemProcedures\ControlOfNonconformingProducts)

1. **DOCUMENT CONTROL INFORMATION**
2. **APPROVAL AUTHORITY**

|  |  |  |
| --- | --- | --- |
| REVISED BY | APPROVAL BY | DATE |
| Food Defense/Food Fraud and Food Fraud Team | Food Defense/Food Fraud and Food Fraud Team | February 22, 2018 |