

PRP Template - Food Defense Program

Food Safety & Quality Template · Provided by GIFSQ

Intentional contamination is unlikely; being unprepared for it is inexcusable. This is a proportionate, practical food defense program - vulnerability assessment first, sensible controls second.

Practical advice before you approve this: keep the frequencies realistic. We've seen programs fail because someone wrote 'daily' for a check that needed a lab slot - then nobody did it. Commit to what you'll actually do, then do it.

1. Document control

Field	Details
Document title	PRP Template - Food Defense Program
Document no.	[QA-PRP-013]
Version	[1.0]
Effective date	[YYYY-MM-DD]
Prepared by	[Name / Title / Date]
Approved by	[Name / Title / Date]
Review date	[YYYY-MM-DD]

2. Purpose

To prevent intentional adulteration of food, ingredients and packaging at this site.

3. Scope

Covers the site perimeter, buildings, storage, production, utilities and information systems at [site name].

4. Responsibilities

Role	Responsibility
Food defense team leader	[Title]: owns the plan and the vulnerability assessment.
Security / Site management	Implement access and perimeter controls.
All staff	Challenge strangers; report suspicious behaviour.
IT	Protect process control and recipe systems.

5. Procedure

1. Form a food defense team and complete a vulnerability assessment of each process step and storage area.
2. Control access: locks, badges or escorted entry for production and storage; visitor log and induction for all guests.
3. Secure the perimeter: fencing, lighting, and locked gates where risk justifies it.
4. Restrict access to sensitive areas (ingredient stores, water treatment, control rooms) to authorized staff only.
5. Screen deliveries: check seals, paperwork and condition; reject suspicious loads.
6. Protect bulk liquids, silos and tanks with locks or seals; monitor access.
7. Train staff to recognize and report suspicious behaviour; define exactly who to call.
8. Have an incident response procedure: isolate suspect product, preserve evidence, notify authorities.

6. Monitoring

Every entry dated and initialled by the person who did the check - in our experience, unsigned logs are the first thing an auditor questions.

What is monitored	How	Frequency	Responsible
Access control compliance	Checks of badges, locks, visitor log	Monthly	Security / QA
Delivery seal checks	Recorded at receiving	Each delivery	Receiving

What is monitored	How	Frequency	Responsible
Vulnerability assessment	Full review	Annually or after incident	Team leader

7. Corrective action

When monitoring shows the program slipping, don't just fix the symptom - the follow-up below matters more than the immediate correction.

1. Investigate every security breach; tighten the failed control.
2. Quarantine any product that may have been tampered with; involve authorities where a crime is suspected.

8. Verification

- Annual vulnerability assessment review.
- Food defense included in internal audits; challenge tests (e.g., escorted stranger) where appropriate.

9. Records

- Vulnerability assessment
- Access control records and visitor logs
- Delivery seal records
- Training records
- Incident reports and investigations

Approval and control

Role	Name	Signature	Date
Prepared by	[Name]	[Signature]	[Date]
Reviewed by (QA)	[Name]	[Signature]	[Date]
Approved by	[Name]	[Signature]	[Date]

Keep completed forms for [Define retention period, e.g., 2 years beyond shelf life] at [defined location] - and make sure someone besides you knows where that is.

General use: This template contains no country-specific laws or regulator names and suits any food business — restaurant, catering, food manufacturing, retail, or food service. Adapt temperature limits, legal references, and record-retention periods to your local regulations. Provided by GIFSQ · v1.0 · September 2026