SIGILL®
KVALITETSSYSTEM AB

IP STANDARD | EDITION 2021:1 | VALID FROM 2021-01-01

# IP FOOD

## BASE LEVEL CERTIFICATION

A quality assurance standard for food handling

FOOD SAFETY | TRACEABILITY | PROBITY

**GRAPHIC DESIGN OCH PRODUCTION**
Sigill Kvalitetssystem AB 2021

**CONTACT**

Sigill Kvalitetssystem AB
105 33 Stockholm
Tel: +46 (0)10-184 45 00
www.sigill.se
info@sigill.se

# **CONTENTS** FOOD

# IP FOOD

## IP IS A STANDARD FOR QUALITY ASSURANCE THROUGH THIRD-PARTY CERTIFICATION

IP is a standard for quality assurance, through third-party certification, in the production of food and ornamental plants throughout the entire food chain from primary production to the processing industry. IP is owned and managed by Sigill Kvalitetssystem AB (Sigill Quality Assurance Ltd).

More information can be found on www.sigill.se.

There are three levels of production requirements for most production types – Base level, Sigill level and Additional level. Moreover, there are supplementary modules, able to supplement the certification on some levels. The supplementary modules can also be used by companies without previous IP-certification.

## BASE LEVEL

- Includes requirements based on current legislation in Sweden as well as food safety and animal protection industry guidelines.
- Raw material produced according to the requirements of the Base level are called "Base level raw material/ products".

## SIGILL LEVEL

- Contains all requirements included in the Base level plus additional stricter requirements concerning food safety, animal welfare and environmental responsibility requirements.
- Raw material produced according to the requirements of the Sigill-level are called "Sigill raw material/products".

## ADDITIONAL LEVEL

- Contains all requirements included in the Sigill- level and additional requirements within specific areas.
- Raw material produced according to the production rules of the Additional level are also called "Sigill raw material/ products".

## SUPPLEMENTARY MODULE

Additional obligations within a certain area of legislation that is relevant for the certified operation, but is not part of the core sector within the standard.

## IP GENERAL REGULATIONS - THE FRAMEWORK FOR CERTIFICATION

The Framework IP General Regulations describes for example the requirements on the certification bodies, what qualifications the auditors must possess, how an audit should be conducted and the general requirements for businesses to be certified. A summary of the IP General Regulations can be found at the end of this handbook.

## THE SCOPE OF THE HANDBOOK

Joining the Standard is voluntary. Generally, the regulations are applicable to all areas within the company associated with the certified production.

## REFERENCE DOCUMENTS

SJVFS 2019:8 4 KAP 4 § TABELL A OCH TABELL B
SJVFS 2019:7, BILAGA 1.1- 1.12
SJVFS 2019:7 3 KAP. 2-3§§

## EXTERNAL AUDIT OF THE COMPANY PRODUCTION

During the first three years an external audit will be carried out on site, with advance notice given. Thereafter, audits will be performed every other year. During the audit documentation, written routines and instructions, certifications, journals etc. are checked, and an inspection takes place.
More information on the different types of audits can be found at the back of this handbook and in IP General Regulations.

## SELF-ASSESSMENT

A self-assessment must be conducted every year. This involves going through the current handbook, and any non-compliances should be noted in an action plan. Non-compliances must be addressed as soon as possible. A self-assessment must be conducted even if there are no non-compliances. Those years when an audit is not conducted on site, the self-assessment is checked by the certification body, also called an administrative audit.

## SUPPORTING MATERIALS

To certain criteria, there is a reference to support material available on www.sigill.se. The use of this material is optional.

## APPROVED INSPECTION AND PENALTIES

To pass the audit it is required that any shortcomings are corrected. If the audit is not approved within the time frame, the company is suspended from the certification system or, in worst case, excluded. More information on penalties and how they are handled, can be found at the end of this handbook and within IP General Regulations.

## THE COMPANY OBLIGATIONS

A company certified according to the IP-standard has the following obligations:

- Current laws and regulations must be followed in the certified business.
- The production rules in place for the certified business, as well as within IP General Regulations, must be followed.
- If the operation require permits or notifications, a copy of these must be presented at the on-site audit.
- There is a duty to implement any changes in production rules or regulations stated in IP General Regulations, as announced by Sigill Kvalitetssystem AB.
- Be responsible for that service providers receive information about their obligations and ensure that regulations are followed.
- Be responsible for that all land, buildings, machinery etc. used by the certified company meet the standards, even if they are owned by another company.
- Participate in and facilitate company audits. This also applies to unannounced audits.
- There is a duty to notify the certification body of any planned changes in production, which may be important for certification (e.g. change of ownership and business expansion).

- There is a duty to notify the certification body if the com pany has been forced to withdraw a product.
- Allow the certification body to disclose any relevant infor mation about the company, that may affect certification and credibility of the IP-standard, to Sigill Kvalitetssystem AB.

## OPENNESS

Information about certified companies, for instance name and address, are published on Sigill Kvalitetssystem AB website, www.sigill.se, after the company has given its consent.

**RED POINT** are marked with a red oval. These requirements are considered particularly important for food safety, traceability and probity, and thereby the core values of IP standard.
Not complying with these red points is considered particularly serious in terms of credibility and can lead to suspension or ex-clusion.

NEW! **NEW RULES** and regulations that have changed significantly are marked with NEW! in the handbook.

S **SUPPORT DOCUMENTS** www.sigill.se/allmant/stodmaterial

| 1 SELF-ASSESSMENT, DOCUMENT MANAGEMENT | | | | | |
|---|---|---|---|---|---|
| | | | FULFILLED RULE? | | |
| | CONTROL POINT | DETAILED REQUIREMENTS AND VERIFICATION | YES | NO | N/A |
| 1.1 S | The food company must be registered or approved by a competent authority. | a) There is documentation proving registration or approval for the facility(s) covered by the certification.<br>b) Registration of individual well or drinking water facility is available if required by local authorities. | | | |
| 1.2 | Self-assessment of the control points covered by the certification shall be carried out annually or more often in the event of significant changes. An action plan shall be drawn up in the event of any deviations or deficiencies. | a) A dated and signed checklist is available.<br>b) Changes are documented.<br>c) Deviations and shortcomings are noted in an action plan.<br>d) Self-assessment and action plan are approved by the responsible person at the company. | | | |
| 1.3 | There shall be routines for handling documents, including written routines mentioned in this standard. | Documents are<br>- current and adapted to the business being conducted<br>- dated with the date they were last modified<br>- clear. | | | |

## 2 VULNERABILITY

Vulnerability analysis is a method for detecting cheating/food fraud and/or threats/sabotage that are intentional and/or criminally committed acts where possible events can have negative consequences for the business.

| | | | FULFILLED RULE? | | |
|---|---|---|---|---|---|
| | **CONTROL POINT** | **DETAILED REQUIREMENTS AND VERIFICATION** | **YES** | **NO** | **N/A** |
| **2.1**<br>**NEW!**<br>S | There shall be a written vulnerability analysis with regard to food fraud/ deception that covers the certified activity.<br><br>The vulnerability analysis shall be reviewed annually or more frequently in the event of changes in the business.<br><br>*Cheating and food fraud can be, for example, dilution, counterfeiting, exchange of raw materials.* | a) There is a dated vulnerability analysis that includes the following:<br>- description of how the company stays up to date on which foods are currently relevant for cheating (e.g. via information from authorities and industry)<br>- if food that there is a risk of being cheated on is handled / mediated within the business<br>- the probability of being affected the conse quences if this happens<br>- preventive work so as not to be affected<br>- opportunities to detect (reception control, supplier assessment, sampling, etc.) and a description of how this is to be applied in the business<br>- direct corrective action to be taken if the company is affected and/or in case of suspicion of fraud/deception.<br>b) Measures taken when the company has been the victim of cheating/fraud are documented. | | | |
| **2.2**<br>**NEW!**<br>S | There shall be a written vulnerability analysis with regard to threats/ sabotage that includes the certified activity.<br><br>*The vulnerability analysis shall be reviewed annually or more frequently in the event of changes in the business.*<br><br>*Internal threats/sabotage can, for example, be intentional contamination with the aim of harming people and/ or the company's reputation. External threats can, for example, be restricted consumption of water/raw materials so that it is not possible to produce food.* | a) There is a dated vulnerability analysis that includes:<br>- A description of how the company stays up to date on external and internal threats (e.g. via information from authorities, industry, newspapers and internal information the risk of internal and external threats and sabotage<br>- the probability of being affected<br>- the consequences if this happens<br>- preventive work so as not to be affected<br>- the possibilities to detect (external protection, visitor control, routines for new hires and terminations, etc.) and a description of how this is to be applied in the business<br>- direct corrective action to be taken if the company is affected.<br>b) Me asures taken when the company has experienced threats/sabotage are documented. | | | |