Process Document

SBP Incident Handling Procedure

Sustainable Biomass Program
sbp-cert.org

Version 1.1

Formal status of document: approved by the SBP Technical Director

Approval date:	4 September 2024
Publication date:	4 September 2024
Effective date:	4 September 2024

Document history

Version 1.0:	24 January 2024 (internal document)
Version 1.1:	4 September 2024 (public document)

In the case of inconsistency between translations, the official English language version shall always take precedence.

Contents

1 Objective and scope of the document

This procedure ensures effective and systematic incident handling by outlining the process to be followed for responding to an incident that may threaten the reputation and/or integrity of the SBP certification scheme, organisation and/or relevant stakeholders. The procedure also includes steps to investigate incidents where fraud is suspected or alleged.

This procedure applies to incidents related to the activities of the SBP certification scheme, SBP Accreditation Body (AB), SBP-approved and applicant Certification Bodies (CBs) and Certificate Holders (CHs).

This procedure does not apply to Appeals and Complaints (refer to https://sbp-cert.org/documents/process-documents/appeals-and-complaints-procedures/).

2 Terms and definitions

Incident Any reported activity, observation, stakeholder comment, or concern that threatens the reputation and/or integrity of the SBP certification scheme and is not already considered under the relevant SBP procedures for Appeals and Complaints.

The response to an Incident by SBP varies depending on priority levels (see 3.3.9) - as opposed to complaints, where a response is always required.

Incidents differ from Appeals in that anyone can report an incident, whereas Appeals are only available to CBs in relation to assessment findings and accreditation/approval decisions.

Incident Handler The SBP Secretariat staff member who received the incident report and logged it in the SBP Salesforce system before forwarding to the Designated Incident Handler.

Designated Incident Handler (DIH) The SBP Secretariat staff member trained on incident handling and with authority to conduct an incident appraisal, plan investigations, review outcomes, and submit a conclusion to close the incident. The default DIH is the SBP Assurance Manager, or SBP Standards Manager in case of potential conflict of interest.

Integrity investigation A type of incident response triggered when an incident or series of incidents represent an integrity risk to the SBP certification scheme. The Secretariat determines if an integrity investigation is warranted. Such investigations can be conducted in collaboration with the AB and CBs and may include a series of incident responses culminating in an investigation report with recommendations to remediate and prevent integrity risks.

Integrity risk A situation likely to result in the violation of SBP requirements, or corruption that threatens the reliability and credibility of the SBP certification scheme, for example, fraud. Major integrity risks (that may trigger integrity investigations) are defined as being, or have a high likelihood of becoming, a systemic problem threatening the credibility and reputation of SBP.

SBP Approval Requirements The various procedures and requirements that are set up by SBP and which the CB must fulfil to be approved for the SBP certification scheme and for maintaining such approval.

Fraud Wrongful or criminal deception intended to result in financial or personal gain.

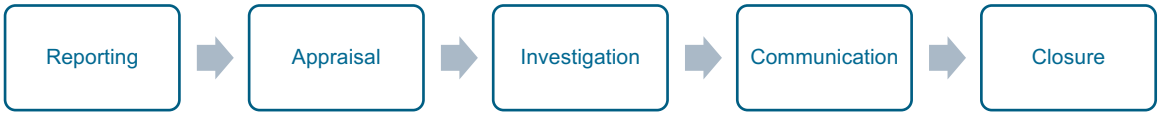
Whistleblower A person who reports an incident regarding any kind of information or activity, where they face risk of retaliation by coming forward. They can report confidentially or anonymously to SBP through the incident handling procedure. Special measures are outlined in this procedure to safeguard their identity.

SBP Assurance Program The sum of all activities implemented for maintaining the integrity and credibility of the SBP certification scheme, including formal accreditation by the AB, SBP training, risk management plan, additional integrity assessments etc.

3 Procedure

3.1 General

Incidents reported to or by the SBP Secretariat or any of its governing bodies are pursuant to the following steps:



3.2 Reporting

3.2.1 Incidents may be reported to SBP through various channels including, but not limited to:

a) Reporting from SBP Secretariat or SBP governing bodies directly through any suitable internal communication channel (e.g., Salesforce, MS Teams, e-mail);

b) Reporting from stakeholders, CHs, AB, CBs, regulatory authorities and/or third parties via the SBP website (https://sbp-cert.org/contact-us/) or by email to info@sbp-cert.org;

c) Anonymous submissions;

d) Confidential submissions; and

e) Reports from the media and/or NGOs brought to SBP's attention.

3.2.2 SBP encourages the reporting of any issues or concerns related to certification and/or accreditation/approval processes associated with the SBP certification scheme. These include, but are not limited to:

a) Allegations of fraud, corruption, unethical behaviour, or misconduct;

b) Concerns regarding questionable business practices or plans;

c) Warnings about areas of risk for the SBP certification scheme, AB, CBs and/or CHs;

d) Potential non-conformities observed related to applicable certification or accreditation/approval requirements.

3.2.3 When an incident is reported to SBP, the Incident Handler shall log it in the SBP Salesforce system ('Complaints and Incidents' module). All SBP Secretariat staff will receive training in this activity. Once the incident is logged, the SBP Salesforce system will send an automatic notification to the SBP Technical Director and Assurance Manager. The Incident Handler may consult with the Assurance Manager before logging the incident.

3.2.4 When dealing with a report from a whistleblower, SBP strives for the protection of whistleblowers and maintains their confidentiality through the following principles:

a) Allowing anonymous and confidential reporting in the incident handling system.

b) Handling all information provided by whistleblowers confidentially to ensure those reporting the misconduct are protected from retaliation.

c) Taking all possible steps to ensure that information provided does not reveal the person's identity but making it clear that complete anonymity cannot be guaranteed in all cases.

d) Never using the evidence provided by whistleblowers directly if there is a risk of revealing their identity. In all possible instances, SBP will collect the evidence again through other means, to avoid linking the evidence with the whistleblower. If that is not possible, SBP will not reveal the evidence in the incident record or any subsequent reports and findings unless it is vital to do so. In such cases, SBP will inform the whistleblower, if their identity is known, about the situation prior to sharing information.

3.3 Appraisal

3.3.1 A Designated Incident Handler (DIH) shall conduct the appraisal. The default DIH is the SBP Assurance Manager. The default DIH may delegate incident handling to another trained DIH.

3.3.2 The appraisal shall be started as soon as possible and no more than seven (7) working days from the date that the incident report was received.

3.3.3 The DIH shall review the SBP Salesforce system entries made by the Incident Handler, particularly those in the appraisal fields of the incident log.

3.3.4 The DIH shall first examine the incident report for possible complaints or appeals, confidential personal and/or human resources issues, and/or whistleblower protection requirements.

3.3.5 If the DIH is unsure if the incident should be a complaint or an appeal, the SBP Technical Director should be consulted for guidance. The person or entity reporting the incident shall be encouraged to submit a complaint or appeal following the relevant SBP procedure. SBP may also offer to handle the complaint or appeal through the appropriate channels, although the final decision rests with the person or entity reporting the incident.

3.3.6 If the incident is a report that shall be handled as a human resources issue (e.g., If an SBP staff member or CB staff member reports an issue related to their own employment or status as a contractor), the DIH shall direct the person or entity reporting the incident to the SBP complaints procedure. The incident log shall then be deleted to protect confidentiality.

3.3.7 If the incident is a report about a CB or CH, the DIH shall inform the person or entity reporting the incident about the CB complaint process, explaining the difference between that and the incident handling procedure, and confirm with the person or entity reporting the incident that they wish to proceed with the incident handling procedure before continuing the appraisal. The final decision rests with the person or entity reporting the incident.

3.3.8 If the incident is reported anonymously or confidentially by a whistleblower, the DIH shall ensure that there are no identifying characteristics in the incident log.

3.3.9 The DIH shall prioritise the incident after analysing all circumstances and consulting with relevant SBP Secretariat staff members. The DIH may also ask the SBP Technical Committee for additional guidance. The SBP response may require urgent investigation (i.e., initiated within 30 days), non-urgent investigation (i.e., initiate within 90 days), investigation through regularly planned assessments, or no action at all.

3.3.10 The DIH shall decide if the AB shall be informed. If this is the case, then the DIH shall send all relevant information to the AB contact person.

3.3.11 The DIH shall determine if the incident is a minor or major incident.

3.3.11.1 The level of the incident is determined by the evaluating the probability/frequency and the consequences for the reputation and/or integrity of the SBP certification scheme.

3.4 Investigation

3.4.1 An investigation is comprised of one or more actions. Each action is referred to as an incident response.

3.4.2 Once the incident response/s is/are assigned, the DIH shall monitor progress and provide support for the investigation. The DIH shall keep the SBP Technical Director regularly informed.

3.4.2.1 Types of incident responses include, but are not limited to:

a) Asking a CB to investigate an allegation against a CH;

b) Asking the AB to add an incident to an AB office assessment of a CB;

c) Asking the AB to schedule a witness assessment;

d) Asking the AB to schedule a desk assessment;

e) Schedule integrity program activity by SBP Assurance team.

CB investigation

3.4.3 The DIH may request CBs to investigate a reported incident.

3.4.4 In such cases, the DIH shall inform the CB, and provide all relevant details (subject to confidentiality).

3.4.5 If the incident constitutes an allegation of non-conformity against a CH, the DIH shall request the CB to provide SBP with a summary of their investigation plan within 10 working days from the SBP request.

3.4.6 CB investigations may not be possible in the following circumstances (note: this is not an exhaustive list):

a) Incidents that include allegations of non-conformance with accreditation/approval requirements (e.g., CB performance issues);

b) Incidents that include more than one CB and/or CH;

c) Incidents related to issues that are outside of the CB's remit.

3.4.7 In the case of clause 3.4.5, SBP may request the CB to provide feedback on the reported incident.

AB investigation

3.4.8 The DIH may request the AB to investigate a reported incident.

3.4.9 The DIH may request the AB to include an incident in an office assessment or conduct a witness assessment and/or desk assessment.

3.4.9.1 When an investigation requires the AB to schedule a witness or desk assessment, SBP and the AB shall take into consideration the existing audit schedule as much as feasible and relevant.

3.4.9.2 The DIH shall request the AB to schedule an extra assessment only if all the following criteria are satisfied:

a) The incident is 'major';

b) The incident requires an assessment as part of the investigation;

c) There are no appropriate CB surveillance assessments available within appropriate timeline.

3.4.9.3 In the case of additional assessments, the costs shall be assigned to the CB unless there is sufficient justification for SBP to cover part or all of the cost (e.g., SBP has requested an additional assessment, or the investigation concludes that there was no CB non-conformity). This shall be determined prior to the AB sending an assessment budget to the CB.

Other Activities

3.4.10 The DIH may request that SBP carries out additional activities as part of the investigation, such as targeted stakeholder consultations, workshops, expert research, innovative projects, data analysis, transaction verification, etc.

Investigation report

3.4.11 The DIH is responsible for the investigation and the analysis of its results. The DIH shall summarise the investigation and confirm the incident level (minor/major).

3.4.12 Using the SBP Salesforce system, the DIH shall issue a report to the SBP Technical Director (minor incident) or the SBP Chief Executive Officer (major incident) for a decision. The report shall include:

a) Summary of the incident;

b) Conclusion on the level of incident;

c) Summary of the investigation;

d) Recommendation on publication and inclusion in the Annual Incident Summary Report;

e) Recommended actions, including lessons learnt and opportunities for continuous improvement.

3.4.13 The recommended actions might require SBP to take immediate actions within their authority to safeguard their credibility, including, but not limited to suspension or termination of an SBP Trade Mark Licence Agreement, publication of new or revised scheme documents.

3.4.14 The SBP Technical Director (minor incident) or the SBP Chief Executive Officer (major incident) shall approve the report.

3.4.15 SBP shall publish an Annual Incident Summary Report on its website.

3.4.16 Once the actions are agreed, the DIH shall assign them to responsible SBP Secretariat staff members, define deadlines, and associated assessment planning requirements, and/or any other actions.

3.4.17 The SBP Assurance Manager shall include a summary of all incidents that occur over the reporting period, the result of the investigation, or their status if ongoing, for consideration as part of the annual SBP Assurance Management Review.

3.5 Communication

3.5.1 For all incidents where the person or entity reporting the incident has provided contact information, SBP shall send an acknowledgement email when the incident is logged in the SBP Salesforce system.

3.5.2 In the case of major incidents, the DIH (or any SBP Secretariat staff member appointed by the DIH) shall inform the person or entity reporting the incident of the outcomes of the investigation once the incident is closed, subject to confidentiality and if contact information has been provided. In cases where communication with the reporter would compromise confidentiality, this requirement is waived.

3.5.3 If the incident is not major, the DIH, at their own discretion or upon request from the person or entity reporting the incident, the DIH may decide to contact the person or entity about the outcome of the investigation, subject to confidentiality.

3.5.4 When a CB requests information about an incident, the DIH shall respond within seven (7) working days. The DIH shall determine the level and type of information on a case-by-case basis and may deny CBs the information request if it would compromise confidentiality and/or the success of the investigation.

Issuing a public statement

3.5.5 If the DIH's investigation concludes that the Incident is based on false claims, technical errors, misunderstanding of SBP requirements and/or irrelevant facts, the DIH may propose issuing a public statement. The DIH shall work with the relevant SBP Secretariat staff members to formulate the statement. If other stakeholders have been mentioned in the Incident, the DIH and relevant SBP Secretariat staff members may consult with the relevant stakeholders. The SBP Chief Executive Officer shall sign off the public statement before publication.

3.6 Closure

3.6.1 Upon recommendation by the DIH, the SBP Technical Director (minor incident) or the SBP Chief Executive Officer (major incident) shall close an incident when all incident responses have been completed, the incident log in the SBP Salesforce system is up-to-date and the recommended actions are completed.

3.6.2 The DIH shall record the date of closure in the SBP Salesforce system.