Integrity Standard Operating Procedures

Reporting and Handling suspected breaches

& Whistle-blower regulations

The Integrity Standard Operating Procedures are an integral part of BSB's Integrity Policy & Procedure Framework, in which applicable principles, dissemination, and related documents are outlined.

1. Introduction

These Integrity SOPs describe the Standard Operating Procedures for reporting and handling suspected integrity breaches.

It replaces the Whistle-blower Regulations, the Complaints- and Appeal Procedure - as far as Integrity complaints are concerned. It is an annex and as such part of BSB's Integrity Policy and system.

The BSB Anti-fraud and -corruption policy paper gives more details and guidelines on specific prevention, detection, investigation and handling of fraud and corruption cases.

Scope

This procedure applies when the alleged perpetrator of misconduct is a representative of BSB including staff, consultants, volunteers and interns. It also applies when BSB and a partner organization have agreed that this procedure would be followed when integrity concerns arise in a joint project.

2. Reporting Integrity Concerns

When it comes to Integrity, staff and anyone who comes into contact with BSB is encouraged to report any suspicion or concern about our representatives' behaviour.

2.1 What to Report?

Any concerns, suspicions, or allegations of integrity breaches, as outlined in the BSB Integrity and Code of Conduct policies and related to Sexual Abuse and Exploitation/ Safeguarding, Fraud, Corruption, Misuse of Power, Conflict of Interest, Anti-Terrorism and Anti-Money Laundering can be reported.

2.2 Why Report?

Allegations of integrity issues should be reported to the organization for two key reasons:

I. For any person affected to receive support and to put a stop to the misconduct,
II. To hold BSB accountable and to help BSB identify and manage risks and trends, which can be used to strengthen the culture of integrity within the organization, e.g. by dismissing staff that doesn't respect BSB's integrity standards.

2.3 Who can Report?

Anyone can report concerns or allegations about the behaviour or BSB representatives or someone linked to BSB. This means that staff, consultants, volunteers, or interns can report, but also third parties like beneficiaries or staff of partner organizations.

2.4 How to Report?

To make a report about an integrity issue, you have different options:

I. Report online using online reporting system from our website https://docs.google.com/forms/d/e/1FAIpQLSfZV87mNAlMS4M-V8Okf0E8ldakfFizjjpHPgOTWVtyBRp7kw/viewform and submit;
II. Speak or email to any of the following persons, whomever you feel most comfortable with:
    - Your manager (your supervisor or higher supervisor)
    - The Integrity Officer via email address: syeshi@bsb.gov.bt
    - HRC/HRM members it to or email to bsb.hrc@bsb.gov.bt
    - You can reach out to the external Whistle-blower Service via the secretariat of ACC via https://www.acc.org.bt/?q=node/1638 or call at 17123412/17123413
III. Report can be made to an independent body by https://www.acc.org.bt/sites/default/files/ComplaitReportingForm.pdf

Note: Do not try to investigate the issue yourself. Your only responsibility is to report the concern or allegation, from there it is the responsibility of the Manager and the Integrity Officer to deal appropriately with the concern.

2.5 The Role of Confidential Advisors

For internal concerns, suspicions, or allegations, Regional Offices and the Global Office in The Hague all have Confidential Advisors, a 'person of trust'. BSB also has an external Confidential Advisor who is not an employee of BSB. You can find names and contact details of all Head of the Divisions and Head of the Organization who are HRC and HRM committee members.

Confidential Advisors are there to listen and support you. Together you can explore whether and what action you can take when you experience or witness misconduct – the decision remains with you. Conversations will be treated confidentially.

3 Protection of complainants/whistle-blowers and others involved

3.1 Protection from Retaliation

BSB considers complaints as vital signals that help the organization fulfill its Duty of Care and ensure that we Do No Harm. We do not tolerate any type of retaliation against complainants, people affected, witnesses, those tasked with handling a case or those supporting the person affected. This includes, but is not limited to dismissal or other unilateral contractual changes, transfers of location or duties, inhibiting professional chances, not granting or imposing benefits (e.g. sick leave, leave days), aggression and violence, bullying, ignoring, excluding, making unfounded or disproportionate criticism about the complainant and their performance, intimidating or threatening the complainant, or equivalent, becauseof the complaint.

When you fear or experience retaliation or breaches of confidentiality, please include this in the initial complaint or reach out to the Manager of your case, the Integrity Officer, or your HR advisor. On a case-by-case basis, suitable measures will be put in place to ensure your

protection. If the retaliatory behaviour amounts to such, it will be considered misconduct in itself.

4 Data Safety

To help protect the confidentiality of integrity issues and the privacy of those involved, the following will apply for emails and documents containing sensitive information:

Wherever identifying details (e.g. names, job title, etc.) are included: mark subject of the email/name of the document as ‘Confidential’ or ‘Strictly Confidential’. In documents, add ‘Confidential’ or ‘Strictly Confidential’ in the header and perhaps add a Watermark ‘Confidential’.
Wherever sensitive, but not directly identifying details are included (e.g. Gender & Integrity Assessments): mark subject of the email/name of the document as ‘Restricted’.
Do not mention identifying details in the subject/title of emails/documents.
Do not share any data with people who are not involved in the response to a case (‘need-to-know rule’), e.g. do not share the original complaint with the Subject of Complaint.
Ensure that emails, folders, documents and notes can only be accessed by those authorized, and password-restrict the access wherever possible.

5. Support to those affected

People affected by misconduct or retaliation might need access to different psychosocial, medical, legal, or security-related services. The Case Manager is in general responsible for overseeing and facilitating the required services, if applicable with the support of the Confidential Advisor, the Integrity Focal Point or the Integrity Officer. The services can be offered either internally or externally, depending on capacity and taking into account the preference of the person affected. Support services are to be paid by the integrity budget of the respective regional office. In exceptional cases, financial support by GO can be requested. Requests will be assessed on a case-by-case basis.

6. Handling of Integrity Concerns or Allegations

Any person who receives a concern or allegation of misconduct of a BSB representative – usually a Health and Safety Focal or Integrity Focal Point – is responsible to provide ‘First Aid’ and to ensure that the complaint is followed up appropriately.

Step 1: Receipt of the complaint (preferably within 24 hrs)

- If in a conversation: ask key questions (what, when, where, who witnessed, etc.), but do not investigate or judge the situation. In case of potentially traumatic incidents (e.g. following sexualized violence), do not ask for details.
- In case of acutepsychosocial, medical, legal, or security needs that cannot wait, make sure that these needs are met (e.g. going to hospital, police, safe place, etc.). Note that in case of serious sexualized violence, such as rape, those affected need to be

able to access medical emergency care within 72hrs of the incident. Only involve people who needto know to help with the response.
- In case of serious incidents (e.g. emergency, child abuse), make a first verbal report to the Integrity Officer and your (Regional) Manager as soon as possible.
- Fill in the reporting form in Annex 1 and send it to bsb.hrc@bsb.gov.bt preferably within 24 hours of receiving the complaint.
- If the report was done in writing: acknowledge receipt of the complaint.

Step 2: Pre-assessment and registration of the complaint (preferably within 48 hrs)

In case of interpersonal misconduct: The Integrity Officer/Integrity Focal Point, in consultation with the HRC, the Integrity Focal Point and Integrity Officer assesses the admissibility and severity of the complaint.

In case of financial misconduct: The Financial Integrity Officer/ Financial Integrity Focal Point, in consultation with the HRC, the Financial Integrity Focal Point and Financial Integrity Officer assesses the admissibility and severity of the complaint.

Admissibility

1) Is the complaint about the behaviour of an BSB representative or someone linked to BSB?
2) Is the complaint about an Integrity issue that falls under the authority of BSB's integrity system?
3) Is there enough information to deal with the complaint?
4) If not, the Integrity Officer will either forward the complaint to those responsible (e.g. Police, Security Advisor or Integrity Officer of partner organization, or line HRC of the accused), or refer the issue back.

Registration

- The Integrity Officer/Integrity Focal Point registers the case, opens a case file including the Report Form and notifies the responsible persons in this case that a complaint was received with a copy to HRC members.
- The Integrity Officer keeps a register of all cases globally.

Step 3: Identification of Case Manager & Case Committee (preferably within 48 hrs)

Based on the pre-assessment of the case, the Integrity Officer and HRC together will assign a case manager and Case Committee.

Case Manager: Where the Manager of the alleged perpetrator is not involved in the allegation, she or he will in general take up the role of Case Manager and will oversee any inquiries or investigations.

Case Committee: most often made up of the Integrity Officer(s), the Integrity focal point(s) and the case manager. Relevant specialists may be added depending on the case.

However, Case Management will be taken up by someone else in either of the following cases:

- The manager is not adequately prepared (trained and/or experienced) to handle the case,
- The manager is in any way – directly or indirectly – implicated in the allegation,
- The alleged perpetrator is the manager,
- Otherwise exceptional case.

Step 4: Case Management ongoing

Risk assessment: The Case Manager conducts a risk assessment (at various levels: safety of the survivor and anyone involved; legal, security, donor and media risks; risks for the project management and implementation) and, in appropriate consultation with the Case Committee, decides/implements measures to mitigate those risks.

Support: The Case Manager ensures that appropriate support services are offered to those affected. This could include psychosocial, medical, legal, or security support services, provided internally (e.g. by Confidential Advisors, Security Advisors, HR advisor) or by external professionals.

Activities: The Case Manager assesses whether a preliminary or full-fledged investigation is necessary and appropriate. If required, the Case Manager can conduct or facilitate a fact-finding inquiry, as long as it does not jeopardize any future investigations. This could include a conversation with the complainant or desk research, without raising profile or informing the alleged perpetrator of the complaint.

Investigation: If an investigation is launched, the Case Manager, in consultation with the Case Committee, drafts the ToR and the Investigation Plan, and appoints the investigation team, usually composed of 2 investigators. At least the lead investigator mustbe trained and experienced in conducting integrity investigations in the given domain (i.e. safeguarding/PSEA, fraud), given the particular complexity and sensitivity of integrity issues.

Reporting: The Case Manager is responsible to notify relevant stakeholders, like local authorities or donors. No identifying details will be shared (unless required by law, for instance in the case of child abuse).

Documentation: The Case Manager is responsible to log all key steps taken, including calls, emails, meetings, investigations, etc. and to keep all documentation related to the case updated and secure (see data safety on page 4).

Step 5: Investigation 1 month (ideally)

- An internal administrative investigation does not replace criminal proceedings, but is BSB's way of ensuring our Duty of Care.
- The Investigation Team, as part of their contract, signs a Confidentiality Agreement [see Annex 4].
- The Investigation Team, in consultation with the Case Manager, revises and adjusts the Investigation Plan if necessary. The Investigation Plan, at a minimum, includes the

documentation and materials to be revised, a list of interviewees, and an investigation timeline to determine the substantiation of the allegation.

- If considered appropriate by the Case Committee, the Subject of Complaint is put on administrative leave for the time of the investigation, unless the risks of doing so (e.g. security risks) are higher than the risk of not putting the SoC on leave.
- The Case Manager, the HoD (if not Case Manager) and, if applicable, HRC are responsible to support the Investigation Team with regards to logistics, accommodation, access to documents and contact to interviewees.
- The Investigation team gathers evidence around the allegation(s) and produces an investigation report including a conclusion on the substantiation of the allegation(s), recommendations, and, if applicable, management observations. The report is shared with the Case Manager and the Case Committee.
- The substantiation of allegation(s) will be assessed on the basis of evidence supporting whether the allegation is found to be substantiated ('proven') or not.

Step 6: Follow-up 1 week

- Based on the investigation report, the Case Manager and Case Committee inform the HRC/Executive Board about disciplinary measures (if any) and, if applicable, organizational improvement measures.
- The investigation is likely to highlight where there has been a failure of supervision and/or a breakdown or absence of controls. The course of action required to improve systems and controls should be documented in the investigation report and implemented when this report is finalized.
- The Executive Board decides whether the EB or the HRC can decide follow-up measures.
- The HRC or Executive Board decides on follow-up measures such as disciplinary or organizational improvement measures.
- The Case Manager is responsible to coordinate the agreed-upon follow-up measures, ideally with a Follow-up plan including the implementation of organizational improvement measures and, if applicable, ongoing support provided to the person affected.
- The HR advisor in HRC is responsible to implement disciplinary measures decided upon by the elected committee, in consultation with the Subject of Complaint's Line Manager. If the allegation(s) were substantiated, a disciplinary hearing is organized, and the case is registered in the Subject of Complaint's personnel records. If the allegation(s) were not substantiated, no data should be stored on the Subject of Complaint's personnel records.
- The Case Manager and, if applicable, the local contact person, is responsible to inform the Subject of Complaint about the result of the investigation and the disciplinary action.
- If the allegation seems to amount to a crime in the country where the case happened, it wasn't reported earlier, and the person affected (if 18+) consents, the case file will by default be handed over to local authorities.
- Where BSB has suffered a loss, full restitution will be sought of any benefit or advantage obtained and the recovery of costs will be sought from the individual or organisation responsible for the loss.

- If the individual or organization cannot or will not compensate for the loss, BSB considers taking legal action to recover the loss
- The Case Manager and, if applicable, the local contact person, is responsible to ensure appropriate follow-up communication with the person affected, e.g. information about the outcome of the investigation.
- The Case Manager is responsible to archive all case documents in a safe way, ensuring that only authorized staff can access the case files.
- Upon implementation of all follow-up measures, the Case Manager, in consultation with the Integrity Officer, closes the case in the Case Register Overview and informs the person affected as well as the complainant (if different from the person affected).
- The level of information shared with the person affected or complainant will be appropriate with regards to the privacy rights of the SoC as well as the right to justice of the person affected. A complainant who is not the person affected might only be informed that the complaint was followed up, and that appropriate measures have been taken, without providing further details. If a Subject of Complaint resigns during an investigation, this will be noted on their personnel records, and indicated when a potential future employer requests a professional reference.

Special cases:

Particularities: This procedure explains the standard procedure. If a particular case requires a different approach because of safety or other needs or wishes of the person affected, or because of particular context or factors, the Case Manager/Integrity Officer will adjust the procedure as required and under due consideration.

Implication/Conflict of Interest: If a person responsible for the response to a case is implicated or has a Conflict of Interest, the tasks are taken up by a person/body in a higher position. For example, if the Integrity Officer is implicated, her tasks might be taken up by the Executive Board

Security: If a case is both an integrity and a security case, it is registered as both, however the Security Advisor and the Integrity Officer coordinate who is in the lead.

High Risk: If a case holds extraordinary risks to the persons involved including well-being, security, reputation, or other risks, the CEO will call on the crisis team consisting of different experts who will be freed up to support the crisis.

Partner: If a case involves a partner organization, but Case Management is taken up by BSB, a representative of the partner organization may take up certain functions in the response, including joining the Investigation Team and/or the Case Committee in relation to the case. Ideally, the organizations should at the beginning of a partnership agree upon a Memorandum of Understanding about the division of responsibilities when integrity cases come up, including the funding of investigations.

7. Disciplinary Measures

Disciplinary measures are regulated per Regional Office HR Manual and HR Manual Global Office (AVR). They range from mandatory training, verbal and written warnings in cases of less severe misconduct and management shortcomings, up to termination of contract in cases of severe misconduct.

Disciplinary measures are decided on a case by case basis following due consideration. As a guideline, 'Severe Misconduct' refers to cases of serious actual or potential harm to people, assets, resources, and funds, or misuse of power or authorities, including – but not limited to – child abuse, sexual abuse and exploitation, misconduct leading to loss of a substantial amount of money, and repeated misconduct.

8. Grievance Procedure

Should a complainant, Subject of Complaint, or someone otherwise involved in a case perceive that their case was not handled appropriately, i.e. that Due Process was not followed, a complaint can be made via the following channels:

A. Externallythrough the ACT Alliance Secretariat who can make an investigation into the manner in which an employer has treated the reporter of a suspected work-related integrity issue.
B. Grievance Procedure laid out in the regional/local HR Manual, if applicable,
C. Through the Grievance Committee for GO. The Grievance Committee follows the procedure laid out for Internal Grievance Procedure, as described in BSB's AVR.

Glossary

Allegation: Assumed misconduct.

Complainant: A person who makes a complaint/report about misconduct to the organization / authorities. This can be the person affected by the misconduct, or a witness / whistle-blower. The term is not to be understood in a negative way.

Complaint: Report of concern, suspicion, or allegation of (potential) misconduct. Concern: Perception of potential misconduct.

Do No Harm: The Principle of ensuring careful consideration so that through our work, no (further) harm is done intentionally or unintentionally.

Duty of Care: The organization's obligation to ensure the safety and well-being of those who come into contact with our staff and programs.

Misconduct: Any behaviour that can be reasonably be understood as breaching the standards of behaviour set out in BSB's Integrity Framework, Code of Conduct and related policies.

Report: See 'Complaint'. Person affected: A person affected by misconduct, e.g. someone who was (sexually) harassed.

SoC (Subject of Complaint): The person who commits the misconduct. When speaking about someone who is suspected to have committed a misconduct, refer to 'alleged perpetrator'.

Survivor/Victim: Both terms can be used to describe persons affected by interpersonal misconduct. While some – especially those who have reached a certain state of recovery – might identify as having 'survived' the distressing incident(s), others feel more 'victimized' by them. One option that doesn't rely on knowing a person's self-identification is to refer to 'persons affected' by misconduct.

Suspicion: Perception, concern or fear about potential misconduct.

Annex 1 Suggested reporting format

A report of a violation/complaint is form-free and can be sent by email. However, this is a suggested complaint/report letter format which can be used. This form should be completed (or adapted) by the person or organization wishing to lodge a complaint with BSB or through a third party. With this form, you can report misconduct of BSB representatives. Fill in as much information as you have at this point – date, time, location, incident, names, … - and send bsb.hrc@bsb.gov.bt as soon as possible. Do not attempt to 'investigate' yourself. Your report will be treated with utmost confidentiality. (Form to be designed and incorporated)

If you are a supervisor who has received a report from an employee or else, fill in this form and send it to bsb.hrc@bsb.gov.bt within 24 hours of receiving the report. All 'sensitive' complaints related to sexual exploitation and abuse, fraud and corruption and gross misconduct will be held securely and handled strictly in line with applicable reporting and investigation procedures.

In case of an emergency, contact the Integrity Officer immediately.

A: General data

Name of the person or organization lodging the complaint: _____

Male/Female: _____

Age: _____

Address: _____

Tel: _____ **email**: _____

Name of the person or organization you wish to lodge a complaint against (if known):

Date of incident: _____

Time of incident: _____

Place of incident: _____

Date of reporting Time of reporting: _____

Brief description of the incident or concern

_____

_____

Name of witnesses (if any/ and if relevant) Supply the names of witnesses and where they can be contacted, if known;

_____

_____

_____

Describe action taken.

If this is a complaint related to sexual exploitation and abuse, please provide detailed information regarding what medical assistance has been provided, what psychosocial care has been provided and whether a report has been made to the Police.

_____

_____

Type and description of allegation

_____

Who is aware of this issue (as far as you know)?

_____

Note: Financial; sexual harassment, exploitation or abuse; Weapons; Drugs and Alcohol; Discrimination; Violence and Aggression; Destruction and Theft, Conflict of Interest, other interpersonal undesirable behaviour (including bullying, intimidation, harassment); other

Annex 2 Confidentiality Agreement Template

Confidentiality Agreement

I understand and agree that in my function as _____ in the case _____, I will have access to confidential information, including but not limited to sensitive personal information from BSB and/or partner staff. To ensure the protection of such information, and to preserve any confidentiality necessary, the Recipient agrees to protect all sensitive information from unauthorized access and not to disclose the confidential information obtained to anyone unless approved in writing by Head of the organization or required to do so by law.

WHEREFORE, I have read and understand this Agreement and voluntarily accept the duties and obligations set forth herein.

Recipient of Confidential Information	**On behalf of BSB**
Name:	Name:
Function:	Function:
Signature:	Signature:
Date:	Date: