

Contents

1	PURPOSE OF THE PROCEDURE	2
2	MOTIVATION FOR CHANGE	2
3	SCOPE.....	2
4	DEFINITIONS/ABBREVIATIONS.....	3
5	SUMMARY OF RESPONSIBILITIES.....	3
6	PROCESS.....	3
6.1	General.....	3
6.1.1	Protection or non-retaliation.....	4
6.1.2	Confidentiality.....	4
6.1.3	Privacy.....	4
6.1.4	Training and Communication.....	4
6.1.5	Local policy and legal requirements.....	4
6.2	Raise an integrity concern	5
6.2.1	Available channels.....	5
6.2.2	Timelines.....	6
6.3	Handling process.....	6
6.3.1	Identification of investigator	6
6.3.2	Investigation	6
6.3.3	Timelines.....	7
6.4	Closure & Reporting.....	7
6.4.1	Closure	7
6.4.2	Reporting	7
7	CORRECTIVE ACTIONS.....	7
8	REFERENCES/ANNEX.....	7

1 PURPOSE OF THE PROCEDURE

'We act with integrity' is one of Bekaert's Values. To speak up, to challenge and to listen are part of our Key Leadership Behaviors, applicable to all of us.

Speaking up to raise an integrity concern as early as possible protects the Bekaert community: our company, our colleagues and our stakeholders. It also helps the company maintain the highest levels of compliance with applicable laws, external and internal regulations, and ethical values. Consequently, every employee has the obligation to report any behavior that deviates from the Code of Conduct, deemed illegal, unethical, or against the interests of Bekaert. We believe that employees should feel safe in reporting, in good faith, any suspected wrongdoing or concerns, and we will safeguard those who speak up (the reporting person).

This procedure describes the processes related to reporting an integrity concern, or (potential) breach of the [Bekaert Code of Conduct](#). It covers the scope, available reporting channels, the follow-up, and protection. Procedure also addresses the European Union's Directive for the protection of persons reporting on breaches of Union law (or 'Whistleblower Protection Directive') approved October 2019.

2 MOTIVATION FOR CHANGE

Internal information.

3 SCOPE

This procedure is mandatory in NV Bekaert SA, its subsidiaries and joint ventures where training was provided on the Code of Conduct.

This scope includes reporting of concerns for non-adherence to the Bekaert Code of Conduct and serious offenses and misconduct in financial, ethical or behavioral matters.

This scope includes e.g.:

- illegal acts
- violation of Bekaert policies including but not limited to anti-trust, privacy, insider trading
- incorrect reporting and accounting
- fraud and theft
- discrimination, hostile environment and sexual harassment
- bribery and corruption
- unauthorized disclosure of trade secrets and confidential information
- damages to safety and health of an individual
- any other conduct which would be likely to harm Bekaert, its reputation or its' employees

Topics not in scope include:

- cyber-security concerns (see SP-Q-36005-BCQA "Cyber Security Resilience Framework")
- personal work-related grievances that are not non-adherences to the Bekaert Code of Conduct, e.g. interpersonal conflict between the reporting person and another employee.

Individuals working at all levels within or outside of Bekaert can report on integrity concern, or (potential) breach. Individuals who can report include:

- employees (whether permanent, fixed-term, or temporary) incl. for example blue and white-collar workers and managers across all entities of Bekaert, senior and executive managers, and members of the board of directors.
- external individuals, including those whose work-based relationship has ended or has yet to begin incl. for example consultants, contractors, trainees, casual workers/agency staff, volunteers, agents and distributors, joint venture partners and employees, vendors and customers.

4 **DEFINITIONS/ABBREVIATIONS**

Identification of any acronyms, abbreviations, or specialized terms used.

ARFC	Audit, Risk and Finance Committee of the Board of Directors of NV Bekaert SA, composed of at least three and maximum five non-executive Directors, including the Chairperson of the Board
Bekaert	Group Bekaert, including all entities trained on the Code of Conduct
CoC	The Bekaert Code of Conduct.
Compliance Committee	composed of CEO, CFO, CHR, General Counsel, VP IA – administered by Head of GRC
GRC	Governance, Risk and Compliance department of Bekaert
HR	Human Resources department of Bekaert
IA	Internal Audit department of Bekaert
JV	Joint venture
Legal	Group Legal department of Bekaert
Reporting person	Natural person who reports information on integrity concern, or (potential) breach

5 **SUMMARY OF RESPONSIBILITIES**

Internal information.

6 **PROCESS**

It is important to disclose relevant information as soon as possible after employees become aware of the integrity concern. Early identification and disclosure will help to protect Bekaert and our employees. Disclosure may be made anonymously, but is not encouraged.

6.1 **General**

Non-retaliation, confidentiality, and privacy principles are continuously applied. Any local legal requirements should be followed at all time.

6.1.1 Protection or non-retaliation

The reporting person will in no way be put at a disadvantage as a consequence of reporting an alleged breach against the Code of Conduct.

Retaliation (any act which occurs in a work-related context, prompted by reporting, and which causes or may cause unjustified detriment to the reporting person) against those who had the courage to speak up is not accepted in any form or manner. Any individual coming forward in such circumstances, regardless of the channel used, will be protected to the full extent possible. Bekaert has an obligation to ensure that employees do not suffer any detriment at work as a result of making a disclosure under the terms of this policy.

Moreover, retaliation is forbidden by multiple laws.

Examples of retaliation because of a raised complaint include:

- Suspension and lay-off
- Demotion or withholding of promotion,
- Transfer of duties,
- Negative performance assessment,
- Disciplinary measures, reprimands, financial penalty
- Intimidation, harassment.

Anyone who violates this non-retaliation regulation, may be subject to disciplinary measures.

This protection or non-retaliation principle includes third parties or facilitators that assist those who speak up, for example colleagues or relatives who could be affected by a disclosure.

6.1.2 Confidentiality

The reporting person's identity or named individuals in the alleged breach will not be disclosed to any person beyond authorized staff members during and after ending the investigation. Where needed, senior management of the concerned department may be informed.

The investigation and outcome is confidential, and shall not be disclosed, except the summary outcome and conclusion to involved management.

Bekaert shall respect the anonymity of a reporting person who does not want to provide his/her name or personal information. The identity of the reporting person will only be disclosed in cases where there is a necessary and proportionate obligation under Union or national law in the context of investigations by authorities or judicial proceedings, in particular to safeguard the rights of defense of persons concerned.

6.1.3 Privacy

Privacy laws principles must be followed.

6.1.4 Training and Communication

Employees within Bekaert are periodically trained on the Bekaert Code of Conduct, which includes a reference to this procedure.

In addition, this policy is published on the intranet on the Code of Conduct page.

6.1.5 Local policy and legal requirements

If there is a local whistleblowing policy, this supplements the Group policy. If conflicting, the strictest procedure will prevail.

If stricter requirements are applicable due to local law, local management shall put these in place.

6.2 Raise an integrity concern

Every concern will be taken seriously. To allow an adequate follow-up process, it is important to document and be as specific and factual as possible. This will add to the credibility of the concern, and the likelihood of confirming the allegation from available resources.

Concerns will be addressed as quickly as possible. Concerns with more substance will be prioritized over concerns without sufficient documentation or information. Concerns without proper substance are more likely to be classified as non-substantiated, and false complaints or malicious complaints could result in disciplinary action towards the reporting person.

6.2.1 Available channels

Bekaert recommends using internal channels prior to external channels to raise a question/concern, and there are multiple internal channels available for this purpose.

Internal reporting will help to identify and address wrongdoing as early as possible. In addition, the internal channels exist to help build confidence and trust in this policy and process.

1. Verbal internal reporting: Discuss potential concern with management

As a first option, each employee is encouraged to report an integrity concern to his or her supervisor, local management, or to his or her HR management. Employment-related concerns should be reported through this channel.

In addition:

- Regional/group IA department representative.
- Group Compliance Manager (English/French/Dutch speaking) via Phone-call to (internal information)

If reported under this procedure, this should be made clear by the employee. Bekaert shall complete and keep accurate records of the meeting/call in a durable and retrievable form, and offer the reporting person the opportunity to review, correct and approve the minutes of the conversation by signing them. The informed management representatives should report the relevant concerns via the e-mail address integrity@bekaert.com, which serves as repository of concerns raised under this procedure.

2. Written internal reporting

As second option, employees are also encouraged to use other internal reporting tools:

Group channels:

- E-mail to integrity@bekaert.com – received by Group Compliance Manager.
- Report on <https://www.bekaert.com/misconduct> - this offers the possibility to raise concerns anonymously. Anonymous concerns will be taken as serious as all other concerns, however this does not allow further follow-up questions and is therefore not encouraged. The entered information will generate an email to integrity@bekaert.com
- Postal address: NV Bekaert SA, Bekaertstraat 2, BE-8550 Zwevegem, for the attention of: Head of Internal Audit

The Group Compliance Manager performs the triage of and has the oversight over the concerns received at Group level. The recipients of the e-mails to integrity@bekaert.com include as well the head of Internal Audit and head of GRC.

Regional channels:

In addition, specific regions have a local in-take channel and follow-up approach:

- North-America:
 - Tel. Internal information.or via www.lighthouse-services.com/bekaert
 - Concern received by regional Finance and HR management representatives, and Group Compliance Manager
- North-Asia:
 - Tel. Internal information.or email to securityhotline@bekaert.com
 - Concern received by head of NAS Security

3. External: local government/police or public disclosure

Employees and stakeholders are encouraged to first contact Bekaert via the available channels to allow Bekaert to quickly validate and address the concern raised.

Alternative external disclosure routes exist as well (government authorities, media), however especially for unproven or false reports, these alternatives may lead to damage to the reputation of individuals and/or Bekaert, and may violate labor or other laws.

RESTRICTED

6.2.2 Timelines

If contact information is available, confirmation of receipt of concern should be sent within seven working days of receipt.

6.3 Handling process

External authorities may be informed and involved as needed during and upon closing of investigation.

6.3.1 Identification of investigator

Investigation may be led by most appropriate employee as agreed with GRC department, depending on the topic; e.g. IA, HR, local management, GRC department representative.

6.3.2 Investigation

The format of the investigation may vary depending on the circumstances. Multiple interviews and fact-finding interviews may take place. Legal department representative may be present and involved to represent Bekaert. Involved persons may choose to be accompanied by another person at will. IT department may also be involved to facilitate the investigation.

During the investigation, the investigator will:

- take concerns seriously and consider them fairly,
- respect this policy for all activities during the investigation,
- communicate as appropriate findings to the reporting person, the individual(s) under investigation and members of the management team and/or external authorities;

6.3.3 Timelines

Three months after the original date of raising the concern, a next communication should be provided to the initiator of concern, including:

- status of the investigation and follow-up steps taken during first three months after raising the concern,
- whether further investigations will follow, and if not, why not.

On a periodic basis, updates may be provided to the reporting person to provide assurance that Bekaert is taking his/her disclosure seriously.

6.4 Closure & Reporting

6.4.1 Closure

Outcome of the investigation for material cases will be summarized in a summary report listing investigation steps taken and conclusion. The investigators should determine in the conclusion part whether the allegation(s) are (a) founded, (b) not founded or (c) inconclusive (means no true or false of the allegation can be substantiated with the evidence provided or investigated). Investigator will share summary report with applicable management, HR and GRC respecting confidentiality. GRC will archive the report.

Disciplinary measures (e.g. formal training, warning letter, letter of undertaking, dismissal for serious breach) towards employees may be a consequence of the investigation conclusion. Disciplinary measures will be decided by HR and local management together with the local Legal department, and shared with the investigator and GRC department. If an employee stepped forward and reported an activity in which he/she was involved, this will be taken into account when making further investigations and the employee may receive a lighter sanction than if he/she had decided to keep quiet.

Upon closure of the case, where possible GRC will communicate from integrity@bekaert.com to the reporting person on the outcome of investigation, actions taken during the investigation, and if any, disciplinary measures taken. This communication should be as soon as possible after the end date of the investigation. This communication to the reporting person is the end-date of the raised concern.

6.4.2 Reporting

GRC department will maintain an overview of cases with specific categories (e.g. substantiated vs. unsubstantiated concerns, breach vs. no breach).

On a quarterly basis, specific cases will be reported to the Compliance Committee.

On a quarterly basis, the cases may be reported to the ARFC. Based on risk, head of GRC will select which cases will be reported in detail.

7 CORRECTIVE ACTIONS

N/A

8 REFERENCES/ANNEX

SM-C05-A03-BCQA : The Bekaert Code of Conduct
SP-Q-36005-BCQA: Cyber Security Resilience Framework