Whistleblowing / internal alert procedure

1. DOCUMENT CONTROL

1.1 Control

Author	Department	Policy owner	Department
Elke Duden	CMS DeBacker	Gerda Vinckx	Management Office
Frequency revision	Every three years and when a significant change occurs		
Responsibility revision	Board of Directors		

1.2 Approval Board of Directors

Approval	Version n°	Description revision	Date
March 12 2024	1		

1.3 History

Version n°	Date version	Change requested by	Description

Change Mechanism

Any request for change or requests for clarifications are to be addressed to the Policy Owner who will ensure the follow-up.

Proposed changes will be discussed and approved as necessary by the Board of Directors.

Updated Policies will be submitted to a formal approval process usually on an annual basis according to the timetable established. If required, a more frequent review can be scheduled.

2. PURPOSE

An IORP has an important social responsibility in the context of pension accrual. Consequently, good governance of the IORP is one of the essential pillars of the IORP's governance.

Compliance with the IORP's values and objectives, as well as the effectiveness of the IORP's code of ethics and its procedures for handling conflicts of interest or complaints, are promoted when employees,

or other persons, such as beneficiaries or pensioners, are able to report violations or unethical behavior in good faith and confidentially. Consequently, the IORP has established a whistleblowing policy in accordance with the Act of 28 November 2022 concerning the protection of whistleblowers reporting violations of Union or national law (hereafter “Whistleblower Act”). The Whistleblower Act allows reporting by the whistleblower through internal and external channels and will ensure protection of the whistleblower who reported violations or unethical behavior in good faith.

3. PERSONAL SCOPE

All natural persons reporting a potential breach in a work-related context are considered a “whistleblower”.

This procedure applies more in particular with respect to the IORP to the following categories including, but not limited to:

a) Members of the General Assembly;

b) Members of the Board of Directors;

c) Members of other operational bodies (if applicable);

d) The key functions (risk management function, actuarial function, compliance officer and internal auditor) as well as the data protection officer ("Data protection officer" or "DPO");

e) The IORP's service providers, subcontractors and their personnel.

In addition, active and passive members, beneficiaries and pensioners may also file a report insofar as the report relates to financial services, products and markets or to prevent money laundering and terrorist financing.

Finally, the protection against retaliation also applies to:

1. facilitators: a natural person who assists a whistleblower in the reporting process and whose assistance must be confidential;
2. third parties related to the reporting persons who may be victims of retaliation in a work-related context, such as colleagues or family members of the reporting persons;
3. legal entities owned by the whistleblowers, for whom the whistleblowers work or with whom the whistleblowers are otherwise connected in a work-related context.

4. MATERIAL SCOPE

Infringements may relate to the following areas:

(a) Violations of laws and regulations;

(b) financial services, products and markets, prevention of money laundering and terrorist financing, in particular relating to pension benefits;
(c) protection of privacy and personal data, and security of network and information systems;
(d) combating tax fraud;
(e) combating social fraud.

Questions or complaints regarding the accrual or payment of the supplementary pension, are not within the scope of this procedure. Questions may be raised through the channels provided for this purpose within the IORP. Complaints are handled according to the complaints procedure. Reports which, after a preliminary examination, turn out to be questions or complaints will be declared inadmissible.

5. INTERNAL REPORTING

5.1 Whistleblower officer

The whistleblower officer is responsible for the receipt, investigation and follow-up of reports. The whistleblower officer is the first point of contact for the whistleblower and must keep the whistleblower informed of the progress of the procedure. The whistleblower officer must be impartial and independent and may not have any conflicts of interest.

The IORP has appointed its compliance officer as whistleblower officer.

5.2 Procedure

5.2.1 Submitting an internal report

The internal report can be submitted by e-mail or letter. The contact details of the whistleblower officer can be found in Annex I.

The internal report can also be submitted to the J&J Integrity Line:
https://secure.ethicspoint.com/domain/media/en/gui/91305/index.html .

5.2.2 Description of the infringement

The whistleblower describes the (potential) infringement in as much detail as possible to enable the whistleblower officer to take note of the situation at hand. The whistleblower also states his/her identity details. Anonymous reporting under this policy is not permitted.

5.2.3 Procedure

A. Acknowledgement of receipt

The whistleblower officer will send a confirmation of receipt within 7 days of receipt of the internal report. This acknowledgment of receipt shall contain at least a description of the report, the date of receipt and a copy of the report received.

B. Correctness of data

Next, the whistleblower officer will verify the accuracy of the data included in the internal report. The whistleblower officer may request additional documents and/or information. This request by the whistleblower officer will be made using the same communication channels as the one used for the internal reporting or according to the whistleblower's reasonable preference.

C. Admissibility

The whistleblower officer will then decide whether the report is admissible. Here the report must be made according to the legally described procedure that is also included in this policy, as well as related to the material scope of this policy. If the report relates to a subject within the scope of the complaints procedure, the report will be passed on to the person responsible for the complaints policy. This will always be done in compliance with applicable privacy laws.

In case the report is considered inadmissible, the whistleblower will be informed accordingly, including the reasons for being inadmissible.

D. Investigation and assessment

The whistleblower officer will investigate the report and assess whether any action needs to be taken. If so, the whistleblower officer will inform the Board of Directors. If a board member is involved in the report, the General Assembly will be contacted.

E. Decision by the Board of Directors/General Assembly

The Board of Directors and/or the General Assembly will decide on and ensure that appropriate measures are being taken. Any action taken will be recorded in the notification register. The whistleblower officer will be informed by the Board of Directors of the measures taken or the fact that no measures were taken and the reasons for this.

F. Feedback

Next, the whistleblower officer will provide feedback to the whistleblower on the measures taken or not taken. This feedback will be communicated within 3 months following confirmation of receipt. In case no confirmation of receipt was sent, the feedback will be communicated within 3 months following 7 days after receipt of the report. If it is not possible to provide feedback within this 3-month period, the whistleblower officer will inform the whistleblower of this and also state the time frame within which feedback can be provided.

The risk manager and the compliance officer will be informed of the outcome, which will include any measures taken and the reasoning if no measures were taken.

If it does not harm the investigation, the whistleblower officer will also inform the person to whom the report relates. In doing so, the confidentiality of the whistleblower's identity will be guaranteed at all times.

6. CONFIDENTIALITY

The whistleblower's internal report will be made to the whistleblower officer, who will keep a record of the reports received. The record is only accessible by the whistleblower officer. This includes information from which the identity of the reporting person can be directly or indirectly deduced. The identity and any other information may only be disclosed if it is a necessary and proportionate obligation under special legislation in the context of an investigation by national authorities or in the context of judicial proceedings, or also to safeguard the rights of defense of the person concerned. Whistleblowers shall be informed accordingly of such disclosures.

7. REGISTER

Any internal report shall be recorded in the register attached in Appendix 2 within seven days of receipt of the internal report.

The IORP is a data controller with respect to the processing of personal data under this policy. The registration of the report shall at all times respect privacy laws. This register is only accessible to the whistleblower officer. The whistleblower officer will implement the required technical and organizational measures to ensure appropriate safeguards, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Reports may be kept for the entire duration of the contractual relationship (such as but not limited to an employment contract, service level agreement, etc.) with the whistleblower, and in any case no longer than necessary. The name, position and contact details both of the whistleblower and any person to whom the protective measures extend, and of the data subject, where appropriate, the company number, will be kept until the reported breach has passed the statute of limitation.

8. PROTECTION OF THE WHISTLEBLOWER

Any person making use of this whistleblowing policy shall be protected against direct or indirect retaliatory measures or decisions with equivalent effect within the IORP or the person's employer.

Retaliation is defined as any direct or indirect act or omission in response to an internal or external report or disclosure, and which results or may result in unjustified harm to the whistleblower.

Any form of retaliation against whistleblowers, including threats and attempts of retaliation, is prohibited, particularly in the following ways:

1. suspension, dismissal or similar measures;
2. demotion or refusal of promotion;
3. transfer of duties, change of job location, reduction in pay, change in working hours;
4. withholding of training;
5. negative performance evaluation or work reference;

6. imposition or application of a disciplinary measure, reprimand or other sanction, such as a financial penalty;
7. coercion, intimidation, harassement or exclusion;
8. discrimination, adverse or unequal treatment;
9. failure to convert a temporary employment contract into an employment contract for an indefinite period of time, in the event that the employee had the legitimate expectation that he/she would be offered employment for an indefinite period of time;
10. non-renewal or early termination of a temporary employment contract;
11. damage, including damage to reputation, especially on social media, or financial loss, including loss of turnover and income;
12. blacklisting based on an informal or formal agreement for an entire sector or industry, which prevents the person from finding employment in the sector or industry;
13. early termination or cancellation of a contract for the provision of goods or services;
14. revocation of a license or permit.

If a whistleblower experiences any retaliation, a new report on this retaliation may be submitted through the internal and/or external channel.

The whistleblower will be protected as described above insofar the whistleblower had reasonable grounds to believe that the information on reported breaches was true at the time of reporting and that the information was within the scope of this policy.

9. EXTERNAL REPORTING

In addition to the internal reporting channel, the whistleblower may also contact the FSMA's reporting channel at https://www.fsma.be/nl/contactpunt-klokkenluiders.

The IORP tries to encourage whistleblowers to first submit a report through the internal channel. The IORP is the most appropriate point of contact for solving problems or reporting abuses, considering that the IORP knows its own internal workings and can take action quickly and efficiently. This does not mean that the IORP prevents external reporting. The whistleblower is free to opt for an external report via FSMA or any other competent supervisory authority.

10. GENERAL DATA PROTECTION REGULATION (GDPR)

The processing of personal data by the IORP under this policy is subject to the Regulation (EU) 2016/679 (GDPR) and the IORP’s privacy policy.

Personal data transferred or used in connection with this policy will be processed in accordance with GDPR. This will ensure that the whistleblower has all rights of access and modification of personal data under GDPR.

11. DISCLOSURE

The Board of Directors undertakes to disclose the above procedure to any person within the scope of this policy (item 3).

Annex 1: Contact details of the whistleblower officer

E-mail address: elke.duden@cms-db.com

Postal address: Generaal Lemanstraat 55, B-2018 Antwerp

J&J Pension Fund OFP (50177)
Turnhoutseweg 30, 2340 Beerse
CBE 0409.886.861

Annex 2: Register

Date the report was received	Date sending acknowledgement of receipt	Description of the report	Outcome initial investigation (correctness of data, admissible or not and reasoning)	Assessment of the report	Recommendation of the Board/General Assembly/Whistleblower officer	Decision	Measures taken	Date feedback to whistleblower	Item closed