

REUNERT: PROTECTED DISCLOSURES AND WHISTLEBLOWING POLICY

Policy information

<i>Policy applies to:</i>	Reunert Group
<i>Policy owner:</i>	Head of Risk
<i>Policy approval:</i>	Reunert Group Executive Committee
<i>Version:</i>	October 2025

Table of contents

1	Introduction	3
2	Acting in good faith.....	3
3	Reporting and recording of disclosures	4
4	Definition of a “Whistleblower”	5
5	Definition of a “Disclosure”	5
6	Safeguards – harassment and victimisation	6
7	How will Reunert respond?.....	6
8	False disclosures	10
9	The responsible officer	10
10	Creating awareness	10
11	Contact details.....	10
12	Review	10

•

1 Introduction

Reunert is committed to the highest standards of ethical and moral business conduct and reassures Whistleblowers that they will be protected from blame, reprisals or victimisation for disclosures made in good faith.

This policy applies to all companies in the Reunert Group, as well as those entities associated with Reunert that are required to comply with Reunert's policies in terms of their Memoranda of Incorporation or shareholders' agreements (collectively referred to as "Business Units"). Business Units¹ should implement such additional policies as may be appropriate to regulate matters not dealt with herein.

This policy is guided by the Protected Disclosures Act, Act 26 of 2000 and section 159 of the Companies Act No. 71 of 2008.

In complying with the legislation Reunert will:

- ensure the protection of Whistleblowers who submit a disclosure in good faith and use the appropriate reporting channels provided by Reunert;
- strive to create a culture of trust which facilitates the disclosure of information relating to criminal and other unethical or irregular conduct in the workplace;
- provide clear guidelines for the disclosure of such information and protection against reprisals as a result of such disclosure (*Refer Paragraph 6*);
- promote zero tolerance to any criminal and other unethical or irregular conduct within Reunert. Irregular conduct would include inter alia: behaviours which are fraudulent, anti-competitive and collusive, or involve intimidation, bribery or extortion.

In the event that there is an inconsistency between this policy and the provisions of the Protected Disclosures Act, the provisions of the Act will prevail.

2 Acting in good faith

Users of the Reunert whistleblowing channels must act in good faith. Disclosures should be made without malice or revenge or consideration of personal benefit, and the complainant should have a reasonable basis to believe the report to be true.

¹ The terms "company" and "Business Unit" or "BU" is used interchangeably in this policy and both refer to the relevant entity, or sub-entity, as the context requires.

Employees should not raise issues on the whistleblowing line that should normally be dealt by way of the company's existing grievance procedures. Only if these channels have been exhausted, or if the employee has reason to believe that using normal procedures would impact a potential criminal investigation, should the employee use the whistleblowing facility.

Note that the whistleblowing channels and this policy are in addition to existing grievance procedures that are available to employees and do not replace such procedures.

3 Reporting and recording of disclosures

To enhance confidentiality, Reunert has outsourced the management of the Reunert whistleblowing channels and has selected and contracted an independent specialist provider, Deloitte Tip-offs Anonymous. Disclosures to Deloitte Tip-offs Anonymous are handled in accordance with strict protocol by professionally trained personnel.

Disclosures can be made using any one of the following communication channels:

- Use of a dedicated FreeCall number which is 0800 864 703
- Use of one unique e-mail address which is expose@tip-offs.com
- FreePost address: KZN 138, Umhlanga Rocks, 4320
- FreeFacsimile: 0800 00 77 88
- Access to the Deloitte Tip-offs Anonymous website which is www.tip-offs.com

Deloitte Tip-offs Anonymous will ensure that any identifying information (for example e-mail addresses) is removed so that the identities of Whistleblowers remain protected. The identity of a Whistleblower will only be provided to Reunert with the express consent of that Whistleblower.

Written reports are prepared by Deloitte Tip-offs Anonymous and sent via email to the Reunert Head of Risk and Internal Financial Controls who then forwards the tip-off to the relevant executive management representatives of the Group company to investigate and provide feedback, as the Head of Risk and Internal Financial Controls deems appropriate, taking account of the nature of the disclosure. The guidelines for managing and monitoring of reports to be investigated are detailed in paragraph 7.1 below.

4 Definition of a “Whistleblower”

Raising a concern about malpractice within an organisation is seen as whistleblowing.

A Whistleblower could be an employee, a worker², a contractor or any other external party who wishes to bring wrongdoing to the attention of management and the Reunert governance structures. The Reunert whistleblowing channels set out in paragraph 1 are a supplementary reporting mechanism through which to raise concerns if, for any reason, a Whistleblower is uncomfortable with using the normal business channels or dissatisfied with the response from the normal business channels. The system is available for use by any employee working within the Reunert group, workers, contractors or any other external parties.

5 Definition of a “Disclosure”

A disclosure is a reported concern that has been submitted by a Whistleblower, acting in good faith, using any of Reunert’s whistleblowing channels set out in paragraph 1. It does not include issues or concerns raised by employees through normal business channels in an open, non-confidential manner. All disclosure reports will be treated in confidence to the extent that it is reasonable to do so.

Examples of disclosures include:

- conduct which is an offence or a breach of law;
- failure to comply with a legal obligation;
- disclosures related to miscarriages of justice;
- health and safety risks, including risks to the public and employees;
- damage to the environment;
- unauthorised use of company resources;
- possible fraud and corruption;
- sexual, mental or physical harassment;
- serious failure to comply with appropriate professional standards;
- abuse of power, or use of company powers and authority for any unauthorised use or personal gain;
- deliberate breach of company policies and/or procedures;
- racist or gender prejudice or any other form of unfair discrimination;

² A worker is an individual who currently or previously worked for any company in the Reunert Group, independent contractors, consultants, agents and those rendering services to a company in the Reunert Group whilst being employed by a temporary employment service (labour broker)

- other unethical conduct; and
- any of the above that is being deliberately concealed.

6 Safeguards – harassment and victimisation

Reunert is committed to good governance and the support of its employees, workers and other third-party Whistleblowers.

Reunert recognises that the decision to make a disclosure can be a difficult one to make. To the extent that it is under Reunert's control, we are committed to ensure that any Whistleblowers are protected for a disclosure made in good faith.

Retaliation of any kind, or the threat to do so, against any person who, in good faith, submits a disclosure or provides assistance to those responsible for investigating the allegations, is not permitted. Any employee of any of the companies in the Reunert group who retaliates against a person who has submitted a disclosure in good faith, shall be subject to disciplinary action, which could result in dismissal.

7 How will Reunert respond?

7.1 General guidelines

Reunert will respond to all disclosures made as outlined in the table below. The Reunert audit committee will receive a summary of all disclosures received and monitor the outcomes on a regular basis. Other board committees, such as the risk committee and social, ethics and transformation committee, may also receive information on disclosures from time to time, where the disclosures are relevant to the mandate of those committees.

Initial enquiries will be made to decide whether an investigation is appropriate and, if so, what form it should take, subject to the minimum requirements that apply to disclosures from employees and workers, set out in paragraph 7.2.

Where an investigation is appropriate, guidance will be given by Reunert to the relevant Business Unit outlining the minimum requirements expected in terms of carrying out the investigation. This will be done individually on a case-by-case basis. The matters raised will either:

- be investigated internally by management, internal audit, head of risk or through the disciplinary process; or

- be referred to an independent outside service provider with the necessary specialist expertise and experience in dealing with the type of disclosure made.

Some concerns may be resolved by agreed action without the need for formal investigations. If urgent action is required, this will be taken, as far as is practical, before any investigations are conducted. In each instance the Head of Risk and Internal Financial Controls will apply his mind to the relevant circumstances to ensure that individuals who are implicated by reports are not in charge of investigations or responsible for communication

The investigation and the duration thereof will depend on the nature of the matters raised, the difficulties involved and the level of detail of the information provided. If necessary and if the Whistleblower consents thereto, further information will be sought from the Whistleblower.

The investigations will, to the extent that it is possible, be handled in a confidential manner and will not be disclosed or discussed with any persons other than those with a legitimate right to such information.

Whilst acknowledging that each report is different and requires individual attention, guidelines for managing and monitoring of reports to be investigated are as follows:

ACTION	PERSON RESPONSIBLE	TIMELINE
Head of Risk to <u>distribute report</u> to relevant person/persons for investigation: • If allegations relate to an employee who is not a BU Executive³, report is sent to the Segment CEO and at least two of the BU Executives. • If allegations relate to a BU Executive, report is sent to Segment CEO and CFO • If allegations are BU HR related, report is sent to Segment CEO and Group HR Executive.	Head of Risk	Within 72 hours of receiving the report from Deloitte Tip-Offs Anonymous

³ “BU Executive” means a member of the BU’s Executive Committee

<u>Investigation</u> of whistle blowing allegations	BU CEO, BU CFO or another Executive of responsible BU (on the understanding that an implicated individual cannot investigate an allegation against himself/herself and that such allegations will be dealt with by the Group CEO/Group CFO together with the Head of Risk, internal audit or external investigators)	2 weeks after receiving the report from the Head of Risk
BU to <u>communicate</u> the result of the investigation and <u>management action</u> plan (to the extent required) to address reported allegations	BU CEO, BU CFO or another Executive of responsible BU	Written feedback to be provided back to Head of Risk within 2 weeks of finalising the investigation.
Head of Risk <u>to communicate</u> results of investigation to Whistleblower if contact details have been provided by the Whistleblower	Head of Risk	Within 2 weeks of finalising the investigation
BU management to communicate results of investigation to person implicated (if the implicated person is aware of the investigation).	BU CEO, BU CFO or another Executive of responsible BU	Within 2 weeks of finalising the investigation including (if applicable) the institution of any legal/disciplinary procedures etc
Closing off of reported allegations	Head of Risk and BU CEO, BU CFO or another Executive of responsible BU	Head of Risk to monitor progress of management action plan monthly until formal close off
Reporting back to Reunert Group examples / outcomes of reports investigated.	Head of Risk on a 6-monthly basis to report back to BUs outlining examples and outcomes of whistle blowing reports investigated	Every 6 months
Reporting to board committees	Head of Risk	Standing agenda item for relevant committee meetings

Note: Reports relating to the Head of Risk, members of the Reunert Executive Committee, Reunert Head Office Executive, or any member of the Reunert Limited board of directors will be reported and investigated through a separate process to ensure appropriate oversight and independence during the investigative process. The same timelines as set out in the table above will apply to such investigations.

7.2 Specific guidelines for feedback to Whistleblowers who are employees or workers of a company in the Reunert Group

The Reunert Group aims to deal with Whistleblower disclosures as quickly and efficiently as possible, in accordance with the timelines set out in the table above.

Without detracting from the Group's intention to deal with matters within the shortest timeframes that are practical under the circumstances, if a Whistleblower is an **employee or worker** of a company in the Reunert Group, the minimum procedures and timelines set out below must be adhered to, as these are prescribed minimum requirements in terms of the Protected Disclosures Act.

The obligation to provide feedback to an employee or worker, set out below, will not apply if the identity and contact details of the employee or worker are not known, or in the event that any communication will prejudice the prevention, detection or investigation of a criminal offence.

Minimum feedback obligations

- A member of executive management of the affected BU (or the Reunert Group CEO, Group CFO, Head of Risk and Internal Financial Controls and Group HR Executive on behalf of the BU, in the event that the nature of the complaint makes it untenable for the executive management of the BU to deal with the matter) must, within 21 days after the disclosure:
 - decide whether to investigate the matter or not; or
 - refer the disclosure to another person or body if more appropriate;
 - AND
 - inform the employee or worker, in writing, of receipt of the disclosure and the decision to investigate (and a timeframe within which the investigation will be completed, where possible), not to investigate, or to refer the investigation to another person or body.
- If the matter has been referred to another person or body, that party must, within 21 days after the referral:
 - decide whether to investigate the matter or not;
 - AND
 - inform the employee or worker, in writing, of receipt of the disclosure and the decision to investigate (and a timeframe within which the investigation will be completed, where possible), or not to investigate (and the reasons it was decided not to investigate); or

- inform the employee or worker, in writing (including e-mail) that the person was unable to reach a decision and thereafter communicate regularly with the employee or worker regarding the decision and reach and communicate a final decision no later than six months after the disclosure was made.
- The employee or worker will be informed of the outcome of an investigation, on the conclusion thereof.

8 False disclosures

It is a criminal offence for a person to intentionally disclose false information with the intention to, and which does, cause harm.

In the interest of good and ethical governance, Reunert may also take disciplinary action against employees or workers who intentionally disclosed false information with the intention to cause harm, which disciplinary action may lead to dismissal.

9 The responsible officer

The Head of Risk and Internal Financial Controls has overall responsibility for the maintenance and implementation of this policy.

10 Creating awareness

This policy will be supported by a structured education, communication and awareness programme as part of Reunert's broader risk management strategy.

11 Contact details

Requests for further information should be addressed to the Reunert Head of Risk and Internal Financial Controls based at Reunert Head Office.

12 Review

This policy shall be reviewed and updated periodically.

Alan Dickson
Reunert Group Chief Executive Officer
On behalf of Reunert Limited