

Whistle-blower Policy 2024

Whistle-blower policy

DOCUMENT PROPERTIES

Entity	Santam Group
Document owner	Risk Committee
Document name	Whistleblowers policy
Document path	J:\ERM\Policies\Whistleblowers Policy\
Classification	Internal

VERSION CONTROL

Version	Date	Who	Saved as
1	10 December 2020	Helen du Toit	Santam Whistleblowers Policy 2020
2	30 November 2022	Helen du Toit	Santam Whistleblowers Policy 2022
3	29 November 2023	Jerry Chetty	Santam Whistleblowers Policy 2023
4	27 November 2024	Jerry Chetty	Santam Whistleblowers Policy 2024

APPROVALS

Version	Approved by	Date approved
1	Santam Exco	10 December 2019
2	Santam Board	30 November 2022
3	Santam Board	29 November 2023
4	Santam Board	27 November 2024

Whistle-blower policy

TABLE OF CONTENTS

	Page
1. Our leadership position	4
2. Purpose of the whistle-blower policy	4
3. Scope	4
4. What is whistle-blowing?	4
5. What misconduct should be reported?	4
6. To whom should disclosures be made?	5
7. Disclosures to outside parties (externally)	5
8. When disclosures (internally or externally) are protected	6
9. When protection will not be provided	6
10. Disclosure made, what is next?	6
11. Can disclosures be made confidentially?	7
12. Protection of whistle-blowers against occupational detriments	7
13. What to do if you are subjected to an occupational detriment	7
14. Examples of misconduct which must be reported (not an exhaustive list)	8
FREQUENTLY ASKED QUESTIONS	9
15. Annexure A: Definitions	10

Whistle-blower policy

1. OUR LEADERSHIP POSITION

Santam Group ("Group") is committed to preventing, detecting and responding to misconduct within the organisation. To this end, the Group recognises the value and contribution of whistle blowing in achieving this objective. The Group understands that employees and workers may be unaware of the whistleblowing process to follow when they come across information regarding misconduct and in some instances employees and workers may even be reluctant to disclose information for fear of reprisals or occupational detriment. To promote a responsible and protected culture of reporting misconduct, the Group has adopted a Whistle-blower policy, which is aligned to the Protected Disclosures Act 26 of 2000 ("PDA"). The PDA was promulgated to encourage employees and workers to disclose information regarding workplace misconduct in a safe environment, free from any occupational detriment.

2. PURPOSE OF THE WHISTLE-BLOWER POLICY

The purpose of this policy is to:

- Set out guidelines on how to make disclosures of misconduct in a responsible manner;
- Assure those making protected disclosures that they should do so without fearing any reprisals or occupational detriment;
- Provides contact details which employees and workers can use to report incidents of misconduct;
- Assure whistle-blowers that all genuine reports of misconduct will be thoroughly investigated and feedback provided; and
- Provide support and remedies to employees or workers who suffer occupational detriment after making a protected disclosure.

The Group believes that responsible whistle blowing **serves as an early warning system** in detecting misconduct which could prevent and/or minimise any exposure to risks. The Group has therefore provided a safe, easy to access, whistleblowing environment, which all employees and workers can use to report incidents of misconduct; the Group encourages whistleblowing.

3. SCOPE

This policy applies to all employees, workers, contractors, suppliers and all stakeholders interacting with the Group.

4. WHAT IS WHISTLE-BLOWING?

It is the disclosure of information in good faith:

- Regarding any conduct of either (a) an employer, or (b) of an employee or worker (whether temporary, permanent, current or former) of the employer,
- Made by an employee or worker (current and/or former) of the employer; and
- Who has reason to believe that the disclosed information shows or tends to show incidents of misconduct as set out below.

5. WHAT MISCONDUCT MUST BE REPORTED?

The listed misconducts are:

- Criminal offences already committed or likely to be committed
- Bribery and corruption
- Unethical behaviour
- A failure or likely failure to comply with legal obligations
- Miscarriages of justice committed or likely to be committed
- The endangering or likely endangering of the health and safety of individuals
- The damage or likely damage to the environment

Whistle-blower policy

- Unfair discrimination as defined in the Employment Equity Act, 1998 (EEA) and Promotion of Equality and Prevention of Unfair Discrimination Act, 2000 (PEPUDA); and
- The concealment or likely concealment of any of the matters referred to above.

Even though protection will be offered in respect of disclosures made after 16 February 2001, employees and workers can also report improprieties that occurred before that date. The Group encourages employees and workers **to make disclosures as soon as reasonably possible** as delays in reporting improprieties may result in evidence being destroyed or tampered with. Whistle-blowers are encouraged to contact the Head: Business Integrity Unit if they are unsure about any of the above.

6. TO WHOM SHOULD DISCLOSURES BE MADE?

To ensure that all reports are promptly dealt with in a fair and objective manner, the Group encourages employees and workers to report incidents of misconduct by using the following channels:

Santam Fraud line (South Africa):	0860 600 767
Santam Fraud line (Namibia):	0800 002 020
E-mail:	forensic.services@santam.co.za
Forensic Cellphone and WhatsApp:	076 921 3347
Postal address:	PO Box 3881, Tyger valley, 7536
Ethics Cellphone and WhatsApp:	066 448 3456
E-mail:	ethicshelpdesk@santam.co.za

Employees and workers are assured that all disclosures made will be investigated and if there is merit to the allegations of wrongdoing, appropriate measures will be taken to remedy the wrongdoing. Such measures will include, but will not be limited to, initiating disciplinary action against those implicated, termination of contracts, laying criminal charges or civil proceedings to recover financial losses incurred.

Whilst it is preferable that the above channels be used to report incidents of misconduct to ensure speedy responses, the following persons within the Group may also be approached with disclosures:

- Your immediate supervisor;
- The Company Secretary;
- Head: Compliance;
- Head: Business Integrity;
- HR Business Partner Lead
- Manager: Employee Relations.

7. DISCLOSURES TO OUTSIDE PARTIES (EXTERNALLY)

Employees and workers are **encouraged to first make disclosures internally** and exhaust all internal reporting mechanisms before considering making disclosures to external parties.

Santam employees also may utilise Sanlam's hotline, which is independently managed by Deloitte to report incidents. Fraud line: **0800 777 543** or email at **sanlam@tip-offs.com** or on their website at www.tip-offs.com or report it to the Insurance Crime Bureau. Fraud line: **0860 002526, SMS 32269** or on **insurance@fraudline.co.za**

Employees and workers can make protected disclosures externally, but protection is available only in these instances:

- If at the time that the disclosure was made, the employee or worker had reason to believe that they will be subjected to an occupational detriment if they made the disclosure internally;
- A disclosure of substantially the same nature was made internally or with the prescribed regulator, but no action was taken within a reasonable period after the disclosure;
- A disclosure was not made internally because the whistle-blower reasonably believed a cover-up was likely and there was no prescribed regulator; and
- The misconduct is of an exceptionally serious nature.

Whistle-blower policy

Where a disclosure based upon the same facts is made to **two or more persons/bodies**, the employee/worker making the disclosure is required to inform each person/body of the fact that a disclosure has also been made to another person/body. In that case, the persons/bodies concerned will ascertain which person or body will conduct the investigation and inform the employee/worker accordingly.

8. WHEN ARE DISCLOSURES (INTERNALLY OR EXTERNALLY) PROTECTED

Employees and workers will enjoy protection for making disclosures if the following requirements are met:

- The disclosure is made in good faith;
- The disclosure is made through the specified channels or to persons mentioned above in paragraph 6;
- An employee or worker reasonably believes that the information disclosed is substantially true; and
- The allegations are not made for personal reward or advantage (this excludes rewards payable in terms of law or in terms of any of the Group's reporting incentive scheme).

9. WHEN WILL WHISTLE-BLOWER PROTECTION NOT BE PROVIDED

Employees and workers who make disclosures will not be protected if:

- The whistle-blower is also implicated in the misconduct;
- The disclosure is false, or the employee or worker ought reasonably to have known that the information is false, and the disclosure was made with the intention to harm the affected party who in fact suffered harm. An employee or worker who makes malicious or false allegations will be considered to have abused this policy and will be subjected to disciplinary action. It is also a criminal offence to intentionally provide false information which results in harm, and such crime is punishable by a fine or imprisonment for up to two years or both;
- The whistle-blower fails to comply with the provisions of this policy, and
- The disclosure is made to an outside third party (externally) without a reasonable cause.

10. DISCLOSURE MADE, WHAT IS NEXT?

As soon as reasonably possible, but in any event within 21 (twenty-one) days after the disclosure has been made, the person within the Group who received the disclosure will, in writing, acknowledge receipt and inform the employee or worker:

- (a) That the matter will be investigated and where possible, indicate the time frames for the investigation; or
- (b) That the matter will not be investigated and the reasons thereof; or
- (c) That the matter will be referred to another person or body if that disclosure could be investigated and dealt with more appropriately by that person or body; or
- (d) That the person to whom the disclosure was made is unable to decide within 21 days whether the matter will be investigated or not. Where a person is unable to decide within 21 days whether they will investigate the matter or not, that person shall, at regular intervals of not more than two months at a time, inform the employee or worker in writing that a decision is still pending.

In addition, as soon as reasonably possible, but **within six months of the disclosure** or the referral, inform the employee or the worker of the decision to:

- (a) Investigate the matter and indicate the timeframes for the investigation if possible; or
- (b) Not to investigate the matter and the reasons thereof.

Where an investigation is conducted, you may be interviewed for further information and you may have to be interviewed. You might even be asked to provide a written explanation or an affidavit. The employee or worker will be informed of the outcome of that investigation, subject to the provision below:

The Group's obligation to acknowledge receipt of the disclosure, to inform the employee or worker of next steps or to inform the employee or worker of the outcome does not arise:

- (a) If the identity and contact details of such employee or worker are not known and
- (b) If it is necessary to avoid prejudice to the prevention, detection or investigation of the allegation.

Whistle-blower policy

11. CAN DISCLOSURES BE MADE CONFIDENTIALLY?

If it is their preference, employees and workers who make disclosures can request that their identity not be disclosed or shared with anyone. The identity of such employees and workers will be treated with the strictest confidence subject to legal provisions. The disclosure of your identity may be required pursuant to a subpoena or in circumstances where the Group is required by law to divulge this information.

In addition, your testimony may be required to prove the case against the accused person or the wrongdoer e.g. testimony in a disciplinary hearing or in a court case. Should this be the case, Forensic Services or the person to whom you have made the disclosure internally will discuss the matter with you first and obtain your permission to disclose your identity.

Where you opt to have your identity withheld, it is advisable that you do not discuss the matter with friends or colleagues. This is to ensure that you also take the reasonable steps to protect yourself.

Employees and workers must also be aware that they can make disclosures anonymously and such disclosures will be investigated. However, employees and workers must take note that it may be difficult to investigate disclosures where the whistle-blower chooses to remain anonymous. It is therefore suggested that in these instances the whistle-blower who chooses to remain anonymous contact Forensic Services again within 7 days should further information be required.

12. PROTECTION OF WHISTLE-BLOWERS AGAINST OCCUPATIONAL DETRIMENTS

The Group is committed to this policy and undertakes to ensure that an employee or worker making a “protected disclosure” will not suffer any occupational detriment. The Group’s assurance to employees and workers making “protected disclosures” is that they will not:

- Be subjected to any disciplinary action;
- Be dismissed, suspended, demoted, harassed or intimidated;
- Be transferred against his/her will;
- Be refused a transfer or promotion;
- Be subjected to a term or condition of employment or retirement which is altered to your disadvantage;
- Be refused a reference, or be provided with an adverse reference from the Group;
- Be denied appointment to any employment, profession or office within the Group;
- Be subjected to any civil, criminal or disciplinary proceedings for the alleged breach of a duty of confidentiality arising out of the disclosure of a criminal offence or information which shows or tends to show a substantial contravention of law;
- Be threatened with any of the actions referred to above; and
- Be otherwise adversely affected in respect of your employment, profession or office, including employment opportunities and work security and the retention of acquisition of contracts to perform work or render service.

13. WHAT TO DO IF YOU ARE SUBJECTED TO AN OCCUPATIONAL DETRIMENT

If an employee or worker or anyone acting on behalf of an employee or worker who is not able to act in his or her own name, reasonably believes that an employee or worker is being subjected to an occupational detriment, they must report this immediately to the Head: Business Integrity.

The employee or worker may also lodge a formal grievance with Human Resources in terms of the grievance procedure.

Anyone who victimises or attempts to discourage an employee or worker from reporting an incident of misconduct commits a disciplinary offence and will be subjected to disciplinary processes.

The Group views such behaviour as a serious form of misconduct.

Whistle-blower policy

14. EXAMPLES OF MISCONDUCT WHICH MUST BE REPORTED (THIS IS NOT AN EXHAUSTIVE LIST)

Misconduct

Misconduct is defined as behaviour not conforming to or in contravention of:

- The Group's values, principles and standards, Code of Ethics or generally accepted good and or responsible business practices.
- Common law and statutory law crimes of the country in which the Group operates.

The Group distinguishes between two types of misconduct:

- Unethical behaviour is the violation of the Group's values, standards, code of ethics or generally accepted good and or responsible business practices.
- Any conduct or suspected conduct or any activity or suspected activity, any action, any omission which causes harm to society and is punishable by law.

See Annexure A for a list of definitions.

Whistle-blower policy

FREQUENTLY ASKED QUESTIONS

What is the origin of the term whistle-blower?

The term whistle-blower derives from the practice of English bobbies who would blow their whistle when they noticed a crime being committed.

What is a whistle-blower?

A whistle-blower is an employee, former employee, or member of an organisation, especially a business or government agency, who reports misconduct to people or entities that have the power and presumed willingness to take corrective action. Generally, the misconduct is a violation of law, rule, regulation and/or a direct threat to public interest – fraud, health, safety violations, and corruption are just a few examples.

Will my report be held in confidence?

Confidentiality will be maintained to the extent possible within the limitations of law. Your identity will, of course, be known to Forensic Services staff members, in order to carry out an investigation. Release of your identity may be required pursuant to a subpoena or in other circumstances where it is required by law to release information. While every endeavor will be made to protect your identity, you should also be aware that it may be necessary in certain circumstances to provide testimony in a court or at a disciplinary hearing. However, before any disclosure is made, Forensic Services will first discuss the matter with you. You should also take necessary steps to protect yourself and should therefore not reveal to anyone that you have reported an incident of misconduct to Forensic Services. Forensic Services will endeavor to take utmost care in protecting your identity and it is therefore advisable that you do not discuss the matter with friends and colleagues.

What if I don't want anyone to know I blew the whistle?

If you wish to remain anonymous, you can call Santam's fraudline on 0860 600 767 and clearly state that you wish to remain anonymous. It is possible that after your initial report further details may be required and it is therefore advisable that you contact the fraudline a week following your first report.

What information should I provide when I make my disclosure?

You should state the facts with as much specific information as possible so that your allegations can be thoroughly investigated. This will include:

- What happened?
- Who was involved?
- When it occurred (e.g. sequence of event, facts, names, dates, etc.)

You should not speculate or draw conclusions, and should be prepared to be interviewed by the person answering the fraudline or follow-up on your e-mail or by an investigator. This will assist to get a better understanding of the information or obtain clarity during the investigation process.

The PDA does not require you to have evidence before blowing the whistle, but does state you must reasonably believe the information is substantially true and such disclosure must be made in good faith.

What happens after I file my whistle-blower report?

Your report will be assigned to a member of Forensic Services. A forensic investigation will be conducted and you may be contacted for further information that might include an interview. You might even be asked to make a sworn statement. Forensic Services will communicate with you on a regular basis unless you have stated clearly that you want to remain anonymous and not be contacted again.

You have the right to be informed of the outcome of your disclosure and the findings of any investigation, although there might be overriding legal or public interest reasons not to do so.

Is there a deadline for filing a whistle-blower report?

No, but it is important to file a report as soon as you have enough evidence to make a good faith report. If you delay evidence can be destroyed which could hamper the success of the investigation.

Whistle-blower policy

15. ANNEXURE A: DEFINITIONS

Term or abbreviation	Definition in the context of this policy
Board	The Board of Directors of Santam Limited.
Business Division/Unit	A business entity that forms part of the Santam Group, but operates independently of the other Business Divisions within the Group.
Business	The Santam businesses that perform the activities of a business subsidiary. Business entities include Santam Group entities, Business divisions and Business units subject to governance oversight requirements provided on a subsidiary level.
Business Unit	Client Solutions, Partner Solutions, Specialist Solutions, Broker Solutions, Santam RE and International and MiWay.
Shared Services	HR, Santam Technology Services (STS), Brand, Procurement and Transformation, Corporate Communication and Santam Experience.
Group CEO	The Group Chief Executive Officer of the Santam Group.
Subsidiary	<p>An investment where the Santam Group exercises a level of control that requires the investment to be consolidated in the Group accounts (either due to equity holding or material influence). It excludes consolidated portfolio investment funds if appropriately approved. In most cases Santam will have a direct or indirect shareholding of more than 50% of the entity's issued capital. For governance purposes, it includes subsidiaries of subsidiaries.</p> <p>A group subsidiary was formerly known as a Group company.</p> <p>It is a grouping of businesses managed by a subsidiary management committee and overseen by a subsidiary/business unit F&R Forum and a QBR Forum which provides assurance to the Santam Limited Board, the Audit Committee, the Risk Committee, Investment Committee, the HRRC and/or the Nominations Committee.</p> <p>Currently this includes:</p> <ul style="list-style-type: none"> • MiWay • Centriq • SSI
Group Entity	A legal entity in the Santam Group, including groupings of such entities designated from time to time as financial conglomerates, insurance groups and insurance sub-groups in terms of the FSR Act, the Insurance Act or a similar Act of another jurisdiction.
Group Exco	The Group Executive Committee of Santam Limited.
Santam	Santam Limited – the controlling company of the Santam Limited Insurance sub-Group and the ultimate holding company of the Santam Group of companies.
Santam Group	Santam Limited and all Group companies comprise of the Santam Group. For avoidance of doubt, this includes the Santam Limited Insurance sub-Group as a whole.
Business integrity	Business Integrity refers to the values of personal integrity, respect for human dignity and the rights of others, honesty and a commitment to do what is right, fair and lawful with which Santam conducts its business. It encompasses the Santam Group commitment to adhering to good governance and compliance with all laws and regulations.
Business ethics	<p>Ethics concerns itself with what is good or right in human interaction. It revolves around three concepts: "self", "good" and "other". Ethical behaviour results when one does not merely consider what is good for oneself but also considers what is good for others.</p> <p>Business ethics is about a conception of what is good (values and standards) that guide the business (self) in its interaction with others (stakeholders).</p>

Whistle-blower policy

Business partner	<p>Business partner refers to any person or entity that renders a service on behalf of the Santam Group. It will refer to but not limited to:</p> <ul style="list-style-type: none"> • All intermediaries (e.g. brokers) • All third parties rendering an outsourced service (e.g. binder holders, underwriting managers, online brokers) • Service providers – shall mean but not limited to contractors, panelbeaters, tow truck operators, retailers, external assessors, builders, plumbers, salvage dealers, security and cleaning services
Cybercrimes	<p>The Cybercrime Act 19 of 2020 criminalises three types of data messages which:</p> <ul style="list-style-type: none"> • Incite damage to property or violence. • Threaten people with damage to property or violence. • Unlawfully contain an intimate image. <p>Cybercrime is defined in Chapter 1 of the Act to include:</p> <p>Revenge pornography which is the non-consensual distribution of a sexually explicit or nude video or photograph.</p> <p>Hacking which is the unauthorised and illegal access to data in a data storage device.</p> <p>Unlawful interception of data meaning the acquisition, viewing, capturing or copying of data of a non-public nature and making that data available to a person, other than the lawful owner.</p> <p>Ransomware meaning malicious software designed to block access to a computer or data storage device until an amount of money is paid.</p> <p>Cyber extortion which occurs when criminals threaten to disable and compromise the accessibility and confidentiality of a target business unless, and until, an amount of money is paid.</p> <p>Malicious communications which include sending data messages which may incite violence, threaten harm, or contains an intimate image of someone.</p> <p>Cyber forgery and uttering occurs when a person defrauds by making, or passing off, false data to the prejudice of another person</p> <p>Cyber fraud is where any person who unlawfully and with the intention to defraud makes a misrepresentation:</p> <p>(a) by means of data or a computer program; or</p> <p>(b) through any interference with data or a computer program as contemplated in section 5(2)(a), (b) or (e) or interference with a computer data storage medium or a computer system as contemplated in section 6(2)(a),</p> <p>which causes actual or potential prejudice to another person, is guilty of the offence of cyber fraud.</p>
Corruption and bribery	<p>Offence of Corruption generally refers to any situation where a person directly or indirectly accepts or offers to accept a gratification from another person/entity, or gives or agrees to give a gratification to any other person/entity for their benefit, or that of another. The giving or acceptance must be done in order to induce the other party to act in an improper manner, in the performance of that individual's/entities' duties. Corruption includes for example the following:</p> <ul style="list-style-type: none"> • Exercising preferential treatment in the awarding of tenders or contracting of service providers <p>Extortion</p> <ul style="list-style-type: none"> • Manipulating the procurement process • Disclosure of confidential information by an employee about his/her company/ department and/or clients • Manipulating the value of assets • Performing favours for relatives and friends

Whistle-blower policy

	<ul style="list-style-type: none"> • Nepotism • Averting the legal consequences of unlawful acts or omissions • Avoiding compliance with laws and regulations • Intentional dereliction of duties as a result of payment or favours received from third parties.
Nepotism	<p>This is a form of favouritism based on acquaintances and familiar relationships whereby someone in an official position exploits his or her power and authority to provide employment opportunities to a family member or friend, even though he or she may not be qualified or deserving.</p> <p>An example would be when a family member or acquaintance is appointed without following due process or has no qualifications or experience for the specific job function. A further example is when a family member receives a supplier contract without following due process.</p>
Extortion	It consists of taking from another some patrimonial or non-patrimonial advantage by intentionally and unlawfully subjecting that person to pressure which induces him or her to submit to the taking.
Intimidation	Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person
Fraud	<p>Fraud is the unlawful and intentional making of a misrepresentation which causes actual prejudice, or has the potential to cause prejudice to another person. For purposes of this policy, and for ease of reference, fraud includes activities involving dishonesty and deception such as the following</p> <p>Misstatements of qualifications, experience and other material facts on job applications and CVs for recruiting purposes</p> <ul style="list-style-type: none"> • Misstatements of material facts on tender documents, proposal or quotation documentation (including BEE ownership) • Identity theft • Forgery and uttering
Insurance crime	Insurance crime is a term used in the Group to define as any conduct or suspected conducted, or any activity or suspected activity, any action, any omission which causes harm to the insurance industry or threatens the financial sustainability of the insurance industry and is punishable by law. These include fraud, theft, forgery, corruption which are very prevalent in the insurance industry.
Money laundering	<p>Money laundering is defined as:</p> <p><i>“an activity, which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds”.</i></p> <p>The Prevention of Organised Crime Act, No. 121 of 1998 (“POCA”) deals specifically with offences relating to the proceeds of unlawful activities and includes “Money Laundering”, “Assisting another to benefit from the proceeds of unlawful activities” and the “Acquisition, possession or use of proceeds of unlawful activities”.</p>
Theft	<p>Theft is the unlawful, intentional appropriation of a moveable, corporeal or incorporeal object which:</p> <ul style="list-style-type: none"> • belongs to, and is in the possession of, another; • belongs to another but is in the perpetrator’s own possession; or • belongs to the perpetrator him- or herself, but is in another’s possession in circumstances under which the possessor has a particular right to possession of the object in question provided that the intention to appropriate the property includes an intention permanently to deprive the person entitled to the possession of the property, of such property.

Whistle-blower policy

Zero tolerance	<p>The Santam Group subscribes to a “zero tolerance” approach to misconduct. In the event that prima facie evidence of criminal conduct is obtained against the offending party; the Santam Group will lodge a complaint with the relevant law enforcement agency for further prosecution. It is important to note that a criminal case will be reported irrespective of whether the Santam Group suffered a financial loss or not.</p> <p>The Santam Group recognises that in certain instances the evidence gathered although not of a criminal nature may amount to contravention of standards, rules or regulations of a regulatory or a governing body. In such an instance the Business Integrity Unit will also report such contraventions to the relevant regulatory or governing body. In addition thereto the Business Integrity Unit, will render such assistance as may be required by the relevant law enforcement agency, governing body or regulatory body for the successful prosecution of the offending party.</p>
-----------------------	--