CfC Stanbic Bank
A member of Standard Bank Group

Policy Name: Whistle Blowing

Level: Group

Type: Governance & Assurance

Policy Owner (In Country): Head, Financial Crime Control

Approved by: Risk Management Committee

Approval date: 30 July 2014

Review date: June 2016

1. Policy statement

The Standard Bank Group Limited (the SBG) actively encourages its employees to embrace its values, especially in respect of the upholding of the highest levels of integrity. Consequently, the obligation exists for SBG employees to report any unlawful, irregular or unethical conduct that they observe. The SBG, in response to cases of whistle-blowing, will apply the highest standards of accountability and corporate governance.

2. Policy scope

The SBG's Whistle-blowing Policy provides for the following:

- Where an employee discovers information, which they in good faith believe shows wrongdoing within the SBG, it should be disclosed without fear of reprisal;
- No employee shall be disadvantaged when reporting legitimate concerns;
- The SBG undertakes to protect employees who in good faith make a report in accordance with the procedures set out in this policy; and
- The SBG will not protect employees who maliciously make false reports and appropriate disciplinary action will be taken, in such cases.

The SBG Whistle-blowing policy is not intended to be utilized for the reporting of petty disputes, grievances, false or misleading disclosures, matters currently under disciplinary enquiry and matters already referred to dispute resolution, arbitration or Labour court.

3. Roles and responsibilities

Group Operational Risk Committee

- Approve and fully endorse this policy.

Group Audit Committee

- Note and supports implementation of this policy;
- Supports implementation of this policy;
- Reviews reports on non-compliance with this policy; and
- Reviews reports on signification matters and consequent management thereof.

Group Financial Crime Control

- Establish an “Office for Whistle-blowing” to handle reporting, investigations, feedback, monitoring and review;
- Implement and update this policy;
- Report on non-compliance with this policy to the Group Audit Committee;
- Provide the monthly whistle-blowing disclosure dashboard to key stakeholders and the Group Audit Committee;
- Perform an annual analysis of the whistle-blowing disclosures made during the past calendar year;
- Act as complainant and the primary Bank’s representative (including the delivery of aggravation and mitigation) in disciplinary enquiries originating from whistle-blowing investigations; and
- Approve requests for exceptions to this policy

Business Unit Management

- Put in place procedures, independent of line management, for the confidential reporting of legitimate concerns;
- Establish standards for reporting concerns to management and Group Financial Crime Control in a secure and timeous manner;
- Implement this policy and develop standards, where applicable, in line with this policy;
- Monitor compliance with this policy;
- Afford appropriate levels of protection to whistle-blowers disclosing in good faith; and
- Report any exceptions to Senior Management and the Whistle-blowing officer; and

- Respect and observe the requirement for Group Financial Crime Control to act as complainant and Bank's representative in whistle-blowing investigation matters that reach disciplinary enquiry.

Line Management

- Accept responsibility in ensuring that all new and current employees are informed of the company's policy and expectations in relation to the confidential reporting (whistle-blowing) process/mechanisms.

4. Whistle-blowing Procedures and Standards

The SBG takes seriously its commitment to our values, business principles, ethical and legal behaviour. For this reason, mechanisms are in place to facilitate the reporting of unethical and/or illegal behaviour, breaches of our values and business principles.

What can be reported?

In terms of these mechanisms, you can report valid concerns regarding the following:

- Conduct which is inconsistent with the SBG's stated vision and values, its code of ethics and policies and procedures, as they may be published and communicated from time to time;
- Violations of law
- Abuse of company resources and assets;
- Danger to the health and safety of any individual; and
- Deliberate concealment of information.

Who can raise a concern?

Any staff member, supplier and contractor, who has a reasonable belief that there is an incident or impending incident which relates to any of the matters specified in the above paragraph, may raise a concern in terms of the procedure reflected below. Concerns must be raised without malice, in good faith, not for personal gain and the individual must reasonably believe that the information disclosed, and any allegations contained in it, are substantially true. The issues raised may relate to a manager, another member of staff, or a group of staff, customers, contractors or vendors.

How are concerns raised?

The SBG wishes to assure the safety of whistle-blowers and therefore undertakes to treat all whistle-blowing reports as confidential. ***The choice between the selection of "confidential" or "anonymous" whistle-blowing is that of the whistle-blower alone.***

Employees may make a confidential report through the Line Management channel, set out below, or alternatively, make either a confidential or an anonymous report through the Whistle-blowing Hotline.

Employees also have the right to report a concern to the local authorities (e.g. police, regulator).

What is confidential whistle-blowing?

A whistle-blower may choose to reveal his or her identity when a report or disclosure is made. Should this be the case, the SBG will respect and protect the confidentiality of the whistle-blower, and gives assurance that it will not reveal the identity of the whistle-blower.

The only exception to this assurance relates to an overriding legal obligation to breach confidentiality. Thus, the SBG is obligated to reveal confidential information relating to a whistle-blowing report if ordered to do so by a court of law.

An advantage for the SBG of a confidential (as opposed to anonymous) report is that it is better placed to investigate the disclosure and request further information to assist the investigation where required.

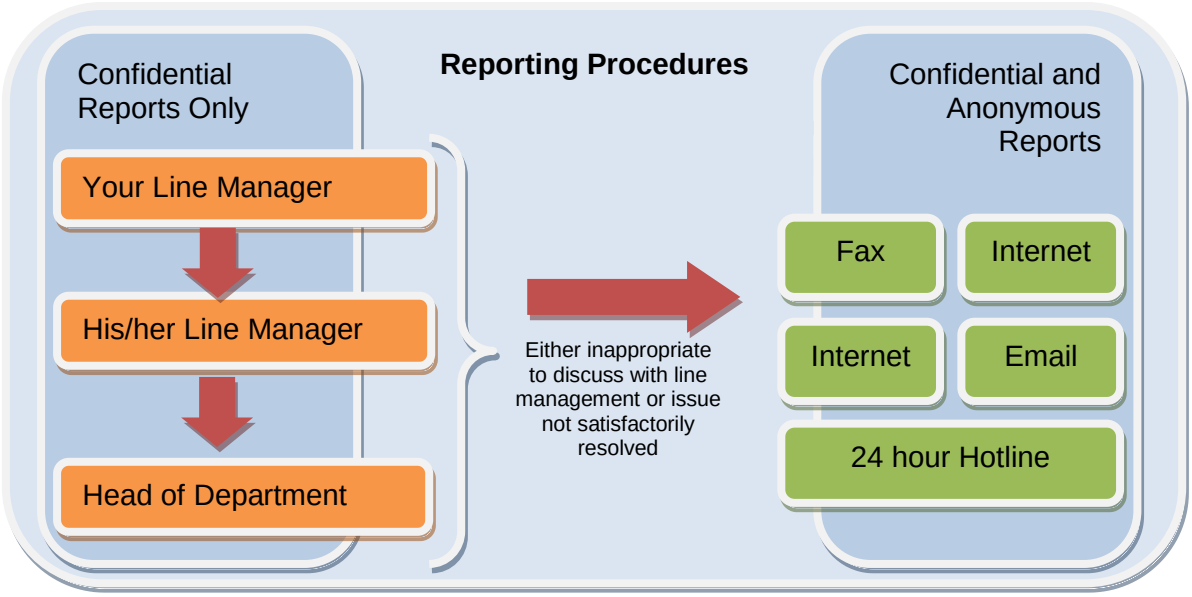
Importantly, the SBG assurance of confidentiality can only be completely effective if the whistle-blower likewise maintains confidentiality.

What is anonymous whistle-blowing?

Alternative to confidential reporting, a whistle-blower may choose not to reveal his or her identity. The SBG has established a Whistle-blowing Hotline, which employees may use to report concerns. The hotline is managed by an independent third party big four audit firm. The systems of the audit firm are set up in such a way that electronic reporting is *non-traceable* through devices such as caller ID and

contractually the audit firm are not permitted to divulge the identity of the caller to Standard Bank (in the event that they become aware of the caller's identity).

The anonymity advantage to the reporter is counter-balanced by the disadvantage to the SBG financial crime investigation, in that it reduces the ability of the investigator to obtain further information relating to the allegations. The anonymous whistle-blower should be careful not to reveal his or her identity to a third party.



If you wish to report an issue, it should be raised, in the first instance, with your line manager. If your line manager is the subject of the matter, it should be reported to his/her line manager or the Head of Department.

Provide as much information as possible, such as names, dates, places and transaction references. Should the line manager find substance in the reported matter, he will escalate the matter in line to GFCC.

The reporting line to be followed is as follows:

- Immediate line manager;
- Head of Department; and

- Group Head of Financial Crime Control.

Significant matters will also be reported to:

- Chairperson, Group Operational Risk Committee;
- Chairperson, Group Risk Oversight Committee;
- Chairperson, Group Risk and Capital Management Committee;
- Chairperson, Group Audit Committee; and
- Chairperson, Board of Directors.

Reporting to Hotline:

You may contact the Whistle-blowing Hotline to make such a report. You may make a confidential report or remain anonymous when making such a report. An operator will answer your call and record the details of the concern you wish to report. During this conversation the operator will request as much information as possible to ensure that the investigators have sufficient information to commence an investigation. Officials of the Whistle-blowing Hotline will submit a report to the designated officials of the Group Financial Crime Control Unit responsible for receiving and actioning such reports.

A list of telephone numbers for every country in which we do business can be found in Appendix B of this Policy. Callers may choose to remain anonymous, but as mentioned previously, are encouraged to provide their names and contact details in the event of further investigation and for the purpose of providing feedback.

However, Callers may re-contact the Whistle-blowing Hotline to request a feedback report from the investigator team and similarly the investigation team may request further information from the Caller by leaving their request for information with the Whistle-blowing Hotline.

Reporting to Group Head of Financial Crime Control:

If these reporting channels have been followed and you still have concerns, or if you feel that the matter is so serious that you cannot discuss it with any of the above, you should contact the Head of Financial Crime Control, whose name and contact telephone number is reflected in Appendix A of this Policy.

Resultant Disciplinary Enquiries

Where, upon completion of the Group Financial Crime Control investigation, it is identified that a disciplinary enquiry will be necessary; the disciplinary enquiry should be initiated and managed by Group Financial Crime Control.

Group Financial Crime Control is deemed to be the primary entity to act and speak on behalf of the Bank (as its appointed representative) in terms of, inter alia:

- The formulation and agreement of charges in consultation with Employee Relations and Human Resources;
- The selection and presentation of witnesses to the disciplinary enquiry;
- The leading and presentation of evidence at the enquiry; and
- The presentation of aggravation, mitigation and answering of any requests for sanction for the alleged misconduct.

The primary purpose of the aforementioned Group Financial Crime Control responsibilities is to ensure a Group wide consistent approach to the consequence management of integrity misconduct related offences.

False or malicious disclosures

Anybody wishing to make a disclosure must guard against making allegations which are false and/or made with malicious intent. The SBG will not protect any employee who makes a report, knowing that the information provided is untrue. In such cases, disciplinary action may be taken against the person concerned and such misconduct will be regarded as serious.

Protection

The SBG will protect the Whistle-blower's identity, if the report or disclosure was made in accordance with the process set out in this policy. The Bank will maintain the confidentiality of the Whistle-blower's identity, unless:

(i) Such person agrees to be identified;

(ii) Identification is necessary to allow the Bank or the appropriate law enforcement officials to investigate or respond effectively to the disclosure;

(iii) Identification is required by law or under the Bank's rules and regulations, where a false accusation has been maliciously made; or

(iv) The person accused is entitled to the information as a matter of legal right or under the Bank's rules and regulations in the disciplinary proceedings.

In such an eventuality, the Bank shall inform the Whistle-blower prior to revealing his or her identity.

Any retaliation, including, but not limited to, any act of discrimination, reprisal, harassment, suspension, dismissal, demotion, vengeance or any other occupational detriment, direct or indirect, recommended, threatened or taken against a whistle-blower because he/she has made a disclosure in accordance with this policy will be treated as gross misconduct and dealt with accordingly.
Whistle-blowers must ensure that they do not make disclosures outside of prescribed channels (e.g. media), or their disclosure may not be protected.

5. More questions?

Will the person be treated differently when raising a concern?
If you have aired a suspicion or concern in good faith, the answer is “no”.

What if the person is not entirely sure, only suspicious?
It can be difficult to have firm evidence of any wrongdoing. It is better to raise any concerns you may have so they can be looked into, rather than ignore them.

What about a personal work-related complaint or concern?
If you have a personal complaint or concern that affects you as an individual, e.g. harassment, this should be raised using the GRG procedures for such matters. Advice on this matter is available from your Business Unit Human Resources. However, the hotline can be used as an alternative.

Will the person raising a concern get into trouble?
If you have raised your concerns as set out in this guide, you will neither be considered a troublemaker nor a disloyal employee for raising your concerns.
If you are involved in the wrongdoing, the SBG will try to ensure that you do not face reprisals from other colleagues for having spoken out. However, you would still have to answer for your own actions and cannot expect immunity from disciplinary or criminal proceedings. The fact that you have disclosed your involvement in any wrongdoing will likely be taken into account.

What if the concerns involve a client of the SBG?

Clients are owed a duty of confidentiality under the SBG policies and local regulations with which we must comply. It is vital to respect this. If you genuinely believe a client is involved in any illegal activity, you must bring this matter to the attention of your local Compliance Head or local Risk Manager. This will ensure that the SBG can deal with the matter lawfully and correctly.

6. Implementation and Review

The policy owner, the Group Head Financial Crime Control, is responsible for creating awareness of the policy, and the related policy standards in this document, including necessary induction, training courses and various forms of communication.
All breaches of the policy and the related policy standards will be recorded in the incident management system.
The policy will be reviewed annually, unless circumstances dictate otherwise.

7. Related information

This policy should be read in conjunction with the following documents:

- Disciplinary Code of Conduct;
- Code of Ethics; and
- Group Reference Guide.

8. Policy administration

Contact person	Bob Ombewa Head Financial Crime Control CfC Stanbic Bank +254203268478 bob.ombewa@stanbic.com
Versions of this policy	V4 – 31 May 2014 – Whistle-blowing Policy
Key words (to assist in locating the policy using the search function)	Whistle-blowing Whistle-blowing Policy Whistle-blowing Policy Standards

9. Appendix A

Whistle-blowing guidance - Internal

The Standard Bank Group nominated Whistle-blowing Officer is:

Name: Karin Griffin Phone: +27 11 636-5396

Alternate to Karin Griffin:

Name: James Roberts Phone: +27 11 636-0514

10. Appendix B

Whistle-blowing contact details (International)

Email: fraud@kpmg.co.za

Fax: +27 12 543 1547

Internet: https://www.surveys.kpmg.com/mmi/2wZTS4P/Link.html

Country	Contact details
Botswana	0800 600 709
Ghana	0800 13237
Kenya	0800 2213 268
Lesotho	800 22222
Malawi	800 05555
Mauritius	800 2122
Mozambique	800 411411
Namibia	+264612942002
Nigeria	234 1271 7739
South Africa	Telephone: 0800 113 443 Fax: 0800 200 796 Post: BNT371, PO Box 14671,

	Sinoville, 0129
Swaziland	+2682404471
Tanzania	999
Uganda	0800200160
Zambia	350377
Zimbabwe	08004100/1/3
Angola	+244 226 432 666
United Kingdom	08000 829 928

11. Revision history

Policy Name	Review Date	Effective Date
Whistle Blowing	31 May 2011	01 June 2011
Whistle Blowing	31 May 2012	01 June 2012
Whistle Blowing	31 May 2013	01 June 2013
Whistle Blowing	31 May 2014	01 June 2014