UAP-Old Mutual Whistle-blowing Risk Policy

UAP OM Policy Owner
Chief Risk Officer

Contact
Erick Kisaka
+254 711 065 670

Date / Version
14/02/2019 /Version 0.8

Proposed date for implementation
Implementation Date is 1 March 2019. For all legal entities other than UAP OM, implementation must be by 1 April 2019. A <Policy Waiver Process> will apply if any Business can demonstrate a justification for any transition arrangements.

Group Operating Manual
All Policies must be read in conjunction with the Group Operating Manual and Quick Reference Guide

Contents

1. Document History

1.1 Revision History

Revision Date	Doc Version	Summary of Changes	Author / Reviewer	Changes Marked?
30 March 2012	0.1	Original draft	C. Rutgers	Y
11 April 20120	0.2	Updated for S Burd comments	S. Burd	Y
28 May 2012	0.3	Reviewed	R Powell	Y
19 June 2012	0.4	Updated for S Burd comments	S Burd	Y
28 June 2012	0.5	Updated for S Burd comments	S Burd	N
4 July 2012	0.6	Updated for MRC comments	C Rutgers	N
11 July 2012	0.7	Updated for MRC meeting held 11 July 2012	S Burd	N
14 February 2019	0.8	Customization for UAP OM Group	S Mwangi	N

1.2 Approvals

This document requires the following approvals.

Name	Title	Doc Version	Approval Signature	Date of Approval
Management Risk Committee (incorporating ExCo Policy Sub Committee, OMEM Policy Owner, SII Compliance Officer)	Chairman (Gary Palser)	0.6	Refer Minutes	11 July 2012
ExCo Risk Committee	Chairman (Ralph Mupita)	0.7	Refer Minutes	17 July 2012
UAP Holdings ARCC	Chairman (Paul Truyens)	0.8	Refer to Miutes	05 March 2019

1.3 Governance Approvals

This document requires the following Board approvals. Please note 2 signatories per Board are required

Board	Representative Name	Doc Version	Approval Signature	Date of Approval
OMLACSA Board Risk Committee	Chairman (Paul Truyens)	0.7	Refer Minutes	31 July 2012
UAP Holdings ARCC	Chairman (Paul Truyens)	0.8	Refer to Minutes	05 March 2019

1.4 Distribution

This document has been distributed to:

Name	Title	Doc Version	Consulted or for Information	Date of Issue
Roelien Powell	Policy Owner	0.7	For information	22 August 2012
	Segment Risk Officers	0.7	For information	20 August 2012
Erick Kisaka	Policy Owner	0.8	For Information	14 February 2019

2. Overview

2.1 Purpose

UAP OM Group is committed to ethical and fair business conduct. Whistle-blowing plays an important part in this.

This policy sets out UAP OM Group requirements for establishing and maintaining whistle-blowing arrangements. Any person making an allegation in good faith is protected from any detriment within UAP OM Group.

2.2 Structure of the Risk Management Policy Suite

UAP OM Group has adopted a consistent approach to Enterprise Risk Management that conforms to good practice and is in compliance with Solvency II requirements. The approach includes the articulation of minimum Principles and Standards as set out in the UAP OM Group risk policies. The structure of UAP OM Group Risk Policies is as follows:

- UAP OM approach to managing each particular risk is set out in a set of risk management Principles.
- Each risk management Principle is supported by a set of Standards setting out how UAP OM has chosen to apply the Principles;
- Measurement of compliance is at the Standards level. Normally, measurement is focussed on exception reporting at a high level;
- The Principles and the Standards, together with the metrics, form the Policy. (Please note that Appendices and documents referenced by this Policy do not form part of the Policy); and
- Processes describing the manner in which the Standards are to be applied are set out in separate Process documentation, linked to the applicable Standard(s) setting out who is accountable for performing these Processes.

2.3 Applicability

This policy applies to UAP OM Group, which includes:

- UAP Holdings and its subsidiaries.

Where UAP OM is not the sole shareholder, the Principles and Standards may be amended to ensure alignment with the shareholder agreement in place. In such cases the spirit and intent of this Policy should be retained to the greatest extent possible.

3. Main Risks Controlled by this Policy

The main risks controlled by this policy include:

- Employees who do not disclose actual or suspected malpractice because of fear of potential detriment; or
- Employees who are not protected from potential detriment when whistle-blows are made in good faith; or
- Concerns disclosed by employees which are not addressed effectively or investigated properly, leading to regulatory and/or legal risk and potential for financial loss and/or brand damage.

4. How Whistle-blowing Risk Arises

The risk arises where employees are unable to disclose genuine suspicions of serious malpractice (examples at Appendix 1) without fear of retribution or detriment within the Group.

5. Mandatory Requirements

5.1. Employees and Senior Management

All employees must act honestly and with integrity at all times and safeguard UAP OM Group resources, tangible and intangible assets and its reputation. Senior management must take reasonable steps to ensure that the culture and ethics of UAP OM reflect this and other UAP OM values. All employees of UAP OM Group are required to co-operate with investigations. Any employee deliberately revealing the presence of an investigation or details contrary to this policy should be subjected to disciplinary action.

5.2. UAP OM Group

UAP OM encourages and supports disclosures of suspected or alleged serious malpractice and has appropriate mechanisms in place to facilitate independent, objective and prompt investigations. This mechanism ensures that the individual making the disclosure is protected from potential detriment as a result of actions by persons internal or external to the Group.

5.3. Whistle-blowing arrangements

5.3.1. Policy

A policy must be implemented in each UAP OM business which specifically communicates Group and UAP OM requirements for whistle-blowing arrangements. Employees who deliberately breach the policy must be subjected to disciplinary action, potentially leading to dismissal. The Head of each Business must ensure that this policy is implemented.

5.3.2. Confidential disclosures

Each business in UAP OM must provide a safe means for whistle-blowers to disclose suspicions of serious malpractice, while guaranteeing as far as is possible anonymity when requested.

All whistle-blower disclosures must be treated in the strictest confidence and all reasonable steps must be taken to protect the identity of the whistle-blower. To be protected as a whistle-blower an individual must:

- Genuinely believe that the knowledge or suspicions disclosed in the whistle-blow are true and relate to serious malpractice. The whistle-blow can relate to past, present or future events.
- Clearly communicate from the outset that a confidential whistle-blowing disclosure is being made.

5.3.3. Allocation of Responsibility

UAP OM must appoint an individual, accountable to the UAP Holdings Board Risk Committee, who is responsible for whistle-blowing and for the protection of whistle-blowers. The person responsible for investigating whistle-blows must be appropriately skilled and have access to all UAP OM records, data and information, including storage on UAP OM owned assets.

5.3.4. Protection of Whistle-blowers

An employee should not suffer detriment as a result of making a whistle-blow – for instance, continued employment, opportunities for future promotion and training of an employee must not be negatively affected because he/she has made a whistle-blow within the terms detailed above.

While protection is provided under this policy, deliberate false or malicious disclosures must not be tolerated. Anyone found making deliberate, false or malicious disclosures must be subjected to disciplinary action, which could lead to dismissal. Giving or accepting an instruction to cover up serious malpractice must not be tolerated and could lead to disciplinary action.

5.3.5. External Advice and Disclosures

Procedures for obtaining independent advice appropriate to each UAP OM business must be detailed in the process documentation supporting this policy. Employees are required to use the internal whistle-blowing process first before disclosing externally, if he/she feels that the whistle-blow has not been taken seriously. Failure to do so should be a disciplinary offence.

5.3.6. Employee Training

Each business in UAP OM must provide regular and relevant training/awareness raising to employees so they are able to identify and disclose suspicions of malpractice; understand UAP OM legal requirements for whistle-blowing; and the protection that must be provided to whistle-blowers. Records of training must be kept to show who received training, the training content and the date the training was received.

5.3.7. Disclosure response plan

Each business in UAP OM must document and implement a whistle-blowing disclosure response plan, clearly detailing the process for investigating whistle-blows including reporting to the Group, and OMA. The process should include timelines where possible (guidelines are detailed in Appendix 2).

5.3.8. Disclosures Relating to the UAP OM CEO and Others

All disclosures must be dealt with via the usual channels except those relating to the CEO which must go through independent channels (for example, the Head of OMA GFS. Disclosures about employees who review disclosures or are part of the management line where disclosures are usually received must be dealt with separately.

Where the disclosure is about a member of the ExCo, the disclosure must be copied to the Head of OMA GFS, who will be responsible for the relevant escalation in line with the GFS Charter and ERM policies and the Group Operating Model.

The independent reporting line Service providers must be notified promptly of any changes that may impact whistle-blow reporting lines, for example names of the CEO and their direct reports.

5.3.9. Legal and regulatory obligations

Each business in UAP OM must determine the extent to which local legal and regulatory duties apply to ensure that they remain locally compliant and can report any conflicts with local legislation.

5.3.10. Management information and assurance of compliance

Each business in UAP OM must provide management information in respect of the

number of whistle-blows received and the number investigated as well as assurance of compliance with this policy to the UAP OM CEO and the Head of Forensics, at least annually.

5.3.11. Compliance

Each business in UAP OM should obtain annual compliance declarations from employees.

5.3.12. Independent Assurance

Group Internal Audit will assess the extent to which risk management and governance practices are effective and that systems of control are functioning as intended, in line with perceived risk.

5.3.13. External reporting

Where appropriate (for example, where criminal behaviour and/or local regulatory breaches have been identified), whistle-blowing events must be reported by GFS to local law enforcement, regulatory bodies or government agencies except where this is impractical or unsafe, in which case, they must be reported to the Head of OMA Forensics . UAP OM must co-operate fully with law enforcement and regulators locally within the bounds of local legislation.

Appendix A: Definitions

A **whistle-blower** is an individual who alerts, via the appropriate channels, UAP OM to serious malpractice or actions that endanger the firm's employees or assets.

Employees, for the purpose of this policy, are permanent staff; fixed term contractors on our payroll; and temporary workers and consultants not on the payroll but engaged for a period of at least one month.

Serious malpractice is defined as behaviour being committed or likely to be committed, including:

- A criminal offence;
- Breach of any legal obligation;
- A miscarriage of justice (for example, recognisable grounds such as fresh evidence, an unreasonable verdict, or a significant misdirection by the judge);
- Endangering health and safety;
- Unethical practice in accounting, internal accounting controls, financial reporting and auditing matters;
- Conduct contrary to UAP OM ethical principles and values; and
- The cover up of any of these.

Serious malpractice does not usually include personal employment grievances (such as bullying, harassment, discrimination) or general complaints. These should be dealt with through the appropriate Human Resources (HR) channels. However, in cases where an employee genuinely considers the issue to be endemic within the firm or their department and no action has been taken in response to a complaint directed to HR, then a whistle-blow may be appropriate.

Confidentiality is where an employee's name is known but will not be disclosed without their consent, unless required by law.

Anonymity is where an employee does not identify him/herself at any stage to anyone.

Appendix B: Guidelines for Implementing Whistle-blowing Arrangements

These guidelines are indicative of the approach that should be taken when implementing whistle-blowing arrangements and responding to disclosures. These guidelines are not definitive - please contact the OMEM Head of Forensics should you need further guidance/information.

1. Policy

The UAP OM policy is aligned with the Group policy, and:

- Give examples of the types of disclosures to be raised and distinguish between whistle-blowing disclosures and grievances.
- Give the option to raise disclosures with line management first and then alternative options if this is not practicable.
- Provide access to an independent disclosure facility, for example a hotline or website.
- Allow whistle-blowing disclosures to be made in confidence.
- Explain when whistle-blowing disclosures can be raised externally, for example to the regulator.
- Forbid (i) reprisals against whistle-blowing disclosures made in good faith; and (ii) making false allegations maliciously.

2. Confidential disclosures

UAP OM encourages employees who have whistle-blowing disclosures to raise these directly with Group Forensic Services. In practice, some employees may (with good reason) feel anxious about identifying themselves, so they must be able to approach someone confidentially. This means that their name will not be revealed without their consent, unless required by law. UAP OM provides access to an independent reporting hotline to facilitate this anonymous disclosure.

3. Employee protection

If employees believe there is malpractice in the workplace then they can make a whistle-blowing disclosure and must be protected from losing their job and/or being victimised by UAP OM.

For employees to be protected as a whistle-blower, they must:

- Be an employee, as defined by this policy;
- Believe that malpractice in the workplace is happening, has happened in the past or will happen in the future;
- Are revealing information of the right type (a 'qualifying disclosure' – see below); and
- Reveal it to the right person, and in the right way (making it a 'protected disclosure' – see below).

A qualifying disclosure includes:

- A criminal offence;
- Breach of any legal obligation;
- A miscarriage of justice (for example, recognisable grounds such as fresh evidence, an unreasonable verdict, or a significant misdirection by the judge);
- Endangering health and safety;
- Unethical practice in accounting, internal accounting controls, financial reporting and auditing matters;
- Conduct contrary to OMEM's ethical principles and values; and
- The cover up of any of these.

For a disclosure to be protected it must be made to the right person, in the right way. The whistle-blower must:

- Make the disclosure in good faith (which means with honest intent and without malice);
- Reasonably believe that the information is substantially true; and
- Reasonably believe that disclosure has been made to the right person.

4. Employee training

UAP OM Group Forensic Services (GFS) and senior managers responsible for managing whistle-blowing arrangements should be trained in the operation of the policy and how to deal with disclosures that are raised. This includes:

- The drivers and values behind effective whistle-blowing arrangements.
- The role of line management.
- Receiving disclosures at a senior level.
- Expectations of confidentiality, for example, whether it was requested, explained or promised.
- Assessing disclosures.
- Addressing the issues raised in the disclosures.
- How to give feedback to and reassure the whistle-blower, including liaison with HR if appropriate.
- Record keeping that complies with data protection procedures and maintaining a chain of evidence should this be required for disciplinary, civil or criminal action.
- Safeguards to protect the whistle-blower ie reprisal against employees making disclosures in good faith is not tolerated; and any reprisal must result in disciplinary action which may lead to dismissal.
- Internal and external accountability, for example failure to follow the procedure - the most effective way for whistle-blowing disclosures to be investigated and the issues resolved is for the internal reporting route to be used. Failure to follow internal options first (for example, by approaching the media before UAP OM) must be considered gross misconduct and must lead to disciplinary action.

New employees must be told about whistle-blowing arrangements when joining UAP OM and all other employees must be reminded of whistle-blowing arrangements at least every other year, this may include:

- Newsletters and other promotional material such as posters.
- Employee surveys.
- Updates on the Intranet.
- Explaining whistle-blowing arrangements when values or ethics are promoted.
- Where appropriate, sharing lessons learned from whistle-blowing disclosures or investigations.

5. Disclosure response plan

Confidential internal disclosures

Suspicions or knowledge of serious malpractice should be dealt with through GFS.

If a whistle-blower chooses to remain anonymous, it is important to ensure that enough information is provided in the whistle-blowing disclosure to facilitate a thorough investigation. However, it helps the investigation significantly if the whistle-blower will speak to the investigators (see below).

External disclosures

As a last resort, a disclosure can be made externally to UAP OM.

Assessing the disclosure

GFS must consider the information in the context of what they know about the particular area or activity and the information the employee provides. From that, and on the assumption that the information is well-founded, GFS should assess:

- How serious and urgent the risk is;
- Whether the disclosure can best be dealt with under the whistle-blowing policy or some other procedure (such as the grievance procedure); and
- Whether the help of or referral to senior managers or a specialist function will be desirable or necessary.

If the information can be treated as a tip-off or a customer complaint and followed up during a routine audit, there may be practical advantages for all concerned. If this appears a realistic way forward, the employee should be informed.

Where an employee formally invokes the whistle-blowing policy and raises a disclosure with GFS, it is helpful if GFS establishes:

- If the employee is anxious about reprisals;
- When the disclosure first arose and, where relevant, what is prompting the decision to speak up now;
- Whether the information is first hand or hearsay;
- Whether confidentiality is sought;
- Whether and when the employee wants feedback; and
- If there is anything else relevant the employee should mention.

Addressing the disclosure

For sensitive issues, the number of people involved in addressing the disclosure should be kept to a minimum and, where the implications are potentially serious or far-reaching, the independence and oversight of the investigation should also be considered. It is also important that, where confidentiality has been promised, it should be respected.

Where specific inquiries need to be made in the area where the whistle-blower works, they should be forewarned so they are prepared to answer questions along with everyone else. By keeping the whistle-blower updated and ensuring they can contact the designated officer if they have any questions, will help manage expectations, pre-empt problems and ensure the process works well.

When considering how to address the disclosure, assume that you will be asked to explain your actions, be it to a regulator, court, supervisory body, shareholders or the media. Also consider whether you should inform an external body (for example, a regulator, a supervisory department or the police) once a serious issue has been identified, either to enlist their assistance or to reassure them and employees that the matter is being addressed properly.

Finally, consider whether the disclosure should be escalated to the Head of OMA, who will coordinate further escalation under the OMA Escalation Policy or Group Operating Manual to GHO.

Investigating the disclosure

Once it is determined that an investigation is required, these steps should be followed:

1. Assign a person responsible for the investigation.

2. Outline an action plan depending on the people and issues involved as well as the severity of the disclosure, considering:
   - What is the allegation?
   - What is the policy regarding these types of allegations?
   - Who is the complainant?

- What position does he or she hold?
- Who is the accused?
- What position does he or she hold?
- Who should be interviewed and in what order?
- Where should the interviews take place?
- What possible issues may arise during the interview process?
- Are there any supervisors or managers that need to be informed?
- Does anyone need to be suspended to stop unlawful behaviour?
- Do computer records need to be frozen?
- Does the IT, Security, the Head of Forensics or HR department need to be consulted?
- What documents should be reviewed?

3. Properly gather and record any evidence in support of the investigation, including e-mails, reports, witness interview statements etc.

4. Report on your findings.

5. Take appropriate action in consultation with appropriate management and HR, for example disciplinary, civil or criminal action.

6. Follow up with the whistle-blower and provide feedback on the outcome of the investigation.

Take remedial action to address control weaknesses and share lessons learned.