Workforce Holdings Limited
(Reg No: 2006/018145/0)

Anti-Fraud, Theft, Corruption, Cyber-crime and Associated Internal Irregularities Policy

1. Background

Workforce Holdings Limited ("the group") wishes to encourage an open and ethical workplace and promote a culture of reporting wrongdoing throughout all its operating subsidiaries and divisions. The Group requires all employees to act honestly and with integrity at all times, to safeguard the group's reputation and to protect company resources. This Policy has being established in line with legal, business and corporate governance requirements.

Workforce Holdings Limited adopts a zero tolerance to inappropriate conduct within the organisation. It is our policy to actively detect fraud or improper conduct and to use every available disciplinary avenue to ensure that the offender is appropriately dealt with.

The Group's **'Risk and Audit Manager'** will independently and objectively investigate all suspected incidents of fraud, theft, corruption, cyber-crime or associated internal irregularities, in line with an approved mandate from the Group's Board of Directors.

2. Purpose of this Policy

All organisations need a system to identify wrongdoing and resolve problems before they negatively affect employees and clients, become too costly or create negative publicity. Where wrongdoing is not identified or reported, this can result in loss of productivity, poor staff morale or job losses for employees and great financial loss for the company. This Policy provides guidance on the meaning of fraud, theft, corruption, cyber-crime and associated internal irregularities and describes how to report, investigate and respond to suspected incidents.

3. Application of this Policy

This Policy applies to all employees within the Workforce Holdings Limited group of companies, including temporary employees, independent contractors, brokers and contracted service providers.

4. Definitions

Fraud is the unlawful and intentional making of a misrepresentation (representing that a fact exists when it does not) which causes actual or potential prejudice to another person. This includes:

- criminal deception for financial gain,
- falsifying the truth of a situation for financial gain, or
- deceiving others by failing or omitting to show the truth of a situation, for financial gain.

Theft is the unlawful and intentional taking of movable property or money belonging to another with the intent to permanently deprive the owner of their rights over the property. This includes:

- taking something of value which does not belong to you without permission from the owner.

The definition for **Corruption** can be found in chapter 1 of The Prevention and Combating of Corrupt Activities Act 12 of 2004. This includes:

- offering, giving or accepting a reward in exchange for doing something illegal or against company policy, or
- agreeing to act in a dishonest manner in exchange for money or personal gain (for example abusing your position of employment to gain an advantage).

The definition for **cyber-crime** can be found in Chapter 8 of the Electronic Communications and Transactions Act 25 of 2002 and forbids:

- any unauthorised access, interception or interference with electronic data, computer-related fraud, forgery and extortion, as well as any attempt to commit or to assist in committing these offences.

An **Associated Internal Irregularity** for purposes of this Policy further defines suspected acts that should be reported to the ***'Risk and Audit Manager'*** for investigation. This includes acts of a material nature involving unethical or dishonest conduct, which could lead to reputational damage or reduce shareholder value in the company. It must be committed against the background of:

a) the employee's general duty to act in the best interest of the employer;

b) the employment contract between the employee and employer;

c) the employee's job description;

d) the employee's performance contract;

e) the Group's established policies.

5. Reporting

All employees have a general duty to act in the best interest of their employer. Any dishonest or unethical conduct should be reported so that an independent and objective investigation can be conducted.

The Protected Disclosures Act 26 of 2000 aims to protect employees from being harassed, victimised or dismissed when they blow the whistle in good faith on wrongdoers in the workplace. The Group's Whistleblower and Whistleblower Protection Policy sets out how suspected unethical conduct must be reported.

The Group will take all reasonable steps to ensure that employees who raise concerns in line with the Whistleblower and Whistleblower Protection Policy are protected from harassment, victimisation or unfair labour practices.

Employees are advised to consult the Whistleblower and Whistleblower Protection Policy for further details of their rights, how they will be protected when reporting unethical conduct and how their report will be dealt with.

The Whistleblower and Whistleblower Protection Policy provides that reports may be made directly or anonymously via an independent whistleblowing process. The options are:

Option 1: Reporting directly to the company's: *'Risk and Audit Manager'*

Option 2: Reporting via an independent external whistleblowing reporting line

6. Management Responsibilities

Management within the Group should report all unethical or dishonest conduct to the ***'Risk and Audit Manager'*** as soon as they reasonably suspect an incident. Where irregularities are reported to, suspected by or brought to Management's attention, the responsible persons should only conduct any initial enquiries necessary to form a reasonable suspicion that an incident has occurred before reporting the matter directly to the ***'Risk and Audit Manager'***.

In order to ensure that investigations are conducted independently and objectively and to ensure that all relevant facts are obtained, managers must not conduct their own investigations, unless it is required to establish a reasonable suspicion.

Investigative work performed by inexperienced individuals may jeopardise the outcome of the investigation or disciplinary or legal action required at a later stage, as evidence needs to be obtained in a legally acceptable manner.

Management is also responsible for:

a. Ensuring effective controls are in place, to assist with the prevention, detection and investigation of possible unethical conduct.
b. Ensuring all employees are made aware of their responsibilities in regard to this Policy.
c. Providing timeous and unrestricted access to the group's functions, records, property and staff.
d. Providing the necessary support to the *'Risk and Audit Manager'* to fulfil her functions.

e. Responding in writing to all recommendations made by the ***'Risk and Audit Manager'***.
f. Ensuring the drafting of acceptable charges and initiating and setting up disciplinary hearings in terms of the Group's Disciplinary Code, based on the ***Risk and Audit Manager's*** investigations

The ***'Risk and Audit Manager'*** has the discretion to, in exceptional circumstances, where a disciplinary matter is of a complex or serious nature, draft charges and appoint an appropriate presenter.

7. Employee Responsibilities

Employees have a responsibility to familiarise themselves with this Policy, including how to report suspected fraud, theft, corruption, cyber-crime or associated internal irregularities. This could include reporting of:

a. Any unethical or dishonest conduct.
b. Any breaches in terms of the Group's policies
c. Any conduct in conflict with the Group's policies and procedures
d. The failure to disclose a conflict of interest
e. Any victimisation or harassment within the workplace
f. Any unauthorised access, interception or interference with electronic data under the Group's control

Employees should approach their line managers or the ***'Risk and Audit Manager'*** in instances where they require guidance on what unethical conduct is.

8. Investigations

Workforce is committed to investigating all unethical or dishonest conduct in an independent and objective manner and to report all suspected criminal conduct to the law enforcement authorities.

In terms of this policy, the Group's line managers do not have authority over the ***'Risk and Audit Manager's'*** decisions to conduct an investigation, nor do they have the right to influence the scope, timing, methodology or direction of particular investigations, or change the contents of reports setting out the results and recommendations of investigations.

During the investigation and disciplinary process an employee cannot be forced to provide information or answers to questions where they may incriminate themselves. In these circumstances, however, a finding and recommendations will be made based only on the evidence presented, with nothing to contradict it.

In line with his mandate, the ***'Risk and Audit Manager'*** is responsible for:

a. Determining the scope and priority of all investigations
b. Deciding who will be responsible for conducting particular investigations. This includes:
    i. decisions to outsource investigations to the Group's line managers or external third parties

ii. Conducting all investigations independently and objectively in terms of the laws of South Africa
iii. Facilitating the internal disciplinary process, where required
iv. Reporting to and liaising with the relevant law enforcement authorities, where required
v. Reporting on the progress and outcomes of investigations to the Group's line managers together with appropriate recommendations for possible further action

Employees may be requested to assist the ***'Risk and Audit Manager'*** with investigations, in line with their general duty to act in the best interest of their employer. This could involve:

a. Making themselves available for interviews and consultations timeously at an agreed venue
b. Assisting in drafting reports or in providing expertise in resolving technical queries relating to their job function
c. Providing access to any company documents, electronic data and records
d. Providing access to any company computers, printers, fax machines and electronic devices including mobile telephones and mobile storage devices
e. Providing access to any electronic user devices attached to company computers, printers, or fax machines
f. Providing access to their workspace on company controlled premises
g. Agreeing to searches of their belongings, clothing or vehicle, when on company controlled premises. The search should take place only if a reasonable suspicion of an irregularity exists and should not disregard the employee's competing right to privacy

9. Suspensions and Disciplinary Procedure

The ***'Risk and Audit Manager'*** may make recommendations to Management to suspend employees if this will facilitate the investigation, reduce the risk to the business or prevent embarrassment to the employee involved.

In line with the Group's industrial relations process, any staff member under investigation may be suspended for a specific period, pending the outcome of the investigation.

Any employee, who fails to comply with this Policy or who intentionally obstructs or misleads the ***'Risk and Audit Manager'*** in the conduct of investigations, could be disciplined and possibly dismissed in terms of the Group's Disciplinary Code.

Misconduct involving fraud, theft or corruption is listed as a dismissible offence by the Group. However, any misconduct by an employee may lead to discipline and possible dismissal.

10. Confidentiality

All information reported to the ***'Risk and Audit Manager'*** will be considered confidential, and personal information will not be disclosed to any individual, unless it is

for purposes of conducting the investigation, reporting to the authorities, or taking disciplinary or legal action.

Any employee who makes a report, or is interviewed during an investigation must keep all information about that investigation, confidential.

11. Rewards

Workforce Holdings Limited does not currently have a formal policy for rewarding whistle-blowers. However, the Group's directors may offer such rewards provided that this is agreed in advance with the ***'Risk and Audit Manager'***.

12. Conclusion

This Policy must be read together with all other applicable policies covered by the Group's Code of Conduct. It must also be read together with the employee's contract of employment, and forms part of the obligations employees have towards the employer and the employer has towards its employees in terms of the employment contract and in terms of the laws of South Africa.

13. Review

These procedures will be reviewed annually to ensure they meet the objectives of the relevant legislation and remain effective for the Group and may be changed at any time at the discretion of the Board of Directors.