Computershare Limited Whistleblower Policy (Incorporating Whistleblower Protection)

1. INTRODUCTION

Ensuring that a process is in place to allow employees to report alleged improper conduct without fear of retribution is an integral component of Computershare's zero tolerance for inappropriate workplace behavior, which may include harassment, illegal acts, cheating, unsafe working conditions, etc. Maintaining an atmosphere of mutual workplace respect and proper business behavior is vital to the integrity and success of the organisation and implementing a structurally sound and business effective whistleblower policy is a significant step towards this end.

Whistleblowing is an important mechanism in the prevention and detection of improper conduct, harassment or corruption. To ensure the theoretical notion of whistleblowing is utilised to its fullest potential for these purposes, guidelines and procedures for reporting, assessing and investigating allegations of suspected improper conduct must be set in place. Computershare must diligently monitor these procedures and ensure that the policies and procedures are effective, and if necessary implement change.

Strategies incorporated in this whistleblower policy (including whistleblower protection) aim to address issues such as reporting, responsibility, confidentiality and effective investigation and resolution. Attention is given to improving the systems and procedures, changing the attitudes of staff and improving the overall integrity and performance of the organisation.

This policy aims to raise awareness of whistleblowing and eliminate the possibility of reprisal and detrimental action in the commercial environment and within Computershare specifically. The measures documented in this policy endeavor to improve the operation of the whistleblowing process, eliminate the risk of reprisal and detrimental action against whistleblowers and to improve the integrity of the organisation as a whole through transparent policies and effective procedures.

1.1 Scope

This policy covers the controls and procedures for dealing with allegations of suspected improper conduct (Whistleblowing). It also addresses the protection and appropriate management of individuals making allegations of suspected improper activity or 'protected disclosures' (whistleblower protection).

The Computershare whistleblower policy is designed to specifically cover *internal* whistleblowing. The key effect of this design feature is that provision is made for the internal reporting of alleged improper activity, to include reporting methods and channels that remain within the organisation and management procedures for alleged improper conduct that are confined to the organisation. In the case of Computershare Limited, provision for external whistleblowing is not warranted, mainly due to the nature and scope of the business and industry regulations.

This policy is applicable to all Computershare employees and related parties and encompasses all subsidiaries under the Computershare brand.

1.2 Background

As has been the case in recent times, governments are progressively introducing whistleblower and whistleblower protection legislation either at a federal or (more commonly) state/provincial level. In addition to this introduction of legislation is the current emphasis on the principles of good corporate governance. Combined, they make a strong argument for implementing whistleblower and whistleblower protection policies.

The trend in whistleblower and whistleblower protection legislation arose from the prevalence in (1) the number of employees (or equivalent) observing improper conduct and subsequently not reporting it, and (2) the number of reprisals

(detrimental action against the whistleblower) resulting from the making of the allegation of suspected improper activity. A recent study out of the United States led researchers to estimate that approximately one third of American employees have observed conduct that they consider to be unethical or illegal in their workplace. Of these, more than half said nothing about the malpractice. Similarly, an Australian study by the Independent Commission Against Corruption (ICAC) estimated that 41 percent of respondents believed that corrupt activity was likely to occur in their workplace. Statistics relating to reprisals are even more supportive. In the same ICAC study, 71 percent of those surveyed expected that people who reported corruption would suffer for reporting it. An American study found even more pronounced results. It showed that two thirds of public and private sector whistleblowers experienced the following forms of reprisals: lost their job (69%), received negative performance appraisals (64%), subjected to increased monitoring (68%), criticised or avoided (69%) and blacklisted from another job in their field (64%).

1.3 Purpose

The purpose of this policy is to outline the controls and procedures for dealing with allegations of suspected improper activity. It provides a framework for management of the whistleblowing process and guidelines on managing the welfare of the whistleblower (whistleblower protection).

This policy aims to establish a system for reporting disclosures of improper conduct or detrimental action by Computershare or its employees. The purpose of this policy is not to act as a stand-alone solution to disclosure of improper conduct, or the protection of the whistleblower, but to complement traditional business communication and increase transparency within the organisation, while facilitating increased confidence in disclosure and assurance of the whistleblower.

More specifically, the purpose of this policy is to:

- Create awareness of the whistleblower policy and whistleblower protection;
- Act as a reference guide to potential whistleblowers wishing to make a disclosure;
- Define the structure of the whistleblower system, including:
    - Reporting System;
    - Roles and Responsibilities;
    - Assessment of Disclosures;
    - Investigation;
    - Post-Investigation Procedures;
    - Whistleblower Protection;
    - Confidentiality; and
    - Review of the Policy.
- Clearly define Computershare's policy on whistleblowing and whistleblower protection;
- Improve the communication and transparency in the processes associated with whistleblowing and assure protection against derogatory consequences, namely reprisals and detrimental action;
- Complement the current communication channels between managers and staff and hierarchical channels flowing right up to the Directors and CEO of Computershare, and
- Provide guidance to all parties involved in either whistleblowing or whistleblower protection.

1.4 Related Documents

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

- Computershare Code of Ethics
- Computershare Employee Handbook

2. DEFINITIONS

2.1 Whistleblowing

For the purpose of this policy, whistleblowing is defined as the deliberate, voluntary disclosure of individual or organisational malpractice by a person who has or had privileged access to data, events or information about an actual, suspected or anticipated wrongdoing within or by an organisation that is within its ability to control.

The term whistleblowing encompasses any disclosure or attempted disclosure of improper conduct (as defined in s2.3 below) by any employee of Computershare regarding any other employee within the organisation.

2.2 Whistleblower

For the purpose of this policy, a whistleblower is defined as any employee of Computershare, who makes or attempts to make a disclosure as defined in s2.1.

2.3 Improper Conduct

For the purpose of this policy, improper conduct is defined as:

(a) harassment (see s2.4);

(b) improper business conduct (see s2.5);

(c) corporate misconduct (see s2.6);

(d) a substantial mismanagement of Computershare resources;

(e) conduct involving substantial risk to public health or safety; or

(f) conduct involving substantial risk to the environment that would, if proven, constitute:

(i) a criminal offence;

(ii) reasonable grounds for dismissing or dispensing with, or otherwise terminating, the services of a Computershare employee who was, or is, engaged in that conduct; or

(iii) reasonable grounds for disciplinary action.

2.4 Harassment

For the purpose of this policy, harassment is defined as offensive, inappropriate conduct that interferes with an employee's working conditions or performance and/or creates a hostile work environment. Sexual harassment may include unwelcome sexual advances; unwelcome requests for sexual favors or unwelcome verbal or physical conduct of a sexual nature. Whether an action is unwelcome is defined by the employee being approached.

2.5 Improper Business Conduct

For the purpose of this policy, improper business conduct is defined as the intentional promise, offer, or gift by any person, directly or indirectly, of an advantage of any kind whatsoever to a person, as undue consideration for themselves, or for

anyone else, to act or refrain from acting in the exercise of their functions, or the intentional request or receipt by a person, directly or indirectly, of an undue advantage of any kind whatsoever, for themselves or for anyone else, or the acceptance of offers or promises of such advantages to act or refrain from acting in the exercise of their functions.

All acts are to be regarded as corruption that involve a person in a position to make decisions using his/her power in that field not in the interest of the organisation he/she represents but to promote his/her personal goals.

2.6 Corporate Misconduct

For the purpose of this policy, corporate misconduct is defined as:

"The unlawful and intentional making of a misrepresentation or inducement of a course of action by deceit or other dishonest conduct, involving acts or omissions or the making of false statements, orally or in writing, with the object of obtaining money or other benefits from or evading a liability to Computershare."

Dishonest activities include, but are not limited to, the following:

- Forgery or alteration of documents (cheques, expense reports, time sheets, agreements, purchase orders, budgets, etc.);
- Misrepresentation of information on documents;
- Misappropriation of funds, securities, supplies, or any other asset;
- Theft, disappearance, or destruction of any asset;
- Improprieties in the handling or reporting of money transactions;
- Authorising or receiving payments for goods not received or services not performed;
- Authorising or receiving payment for hours not worked;
- Any violation of Federal, State, or Local laws related to dishonest activities; or
- Any similar or related activity.

Note: Internal and external fraud perpetrated against clients or shareholders is primarily covered by the Anti-Fraud Policy; however, these can be reported through the whistleblower policy if the whistleblower fears recrimination and wants to take advantage of the protections afforded by the whistleblower policy and the provisions of the whistleblower policy apply to the event being reported.

2.7 Protected Disclosure

For the purpose of this policy, protected disclosure is defined as any good faith communication that discloses or demonstrates an intention to disclose information that may evidence (1) an improper activity or (2) any condition that may significantly threaten the health or safety of employees or the public, if the disclosure or intention to disclose was made for the purpose of remedying that condition.

2.8 Detrimental Action

For the purpose of this policy, detrimental action is defined as:

(a) action causing injury, loss or damage;

(b) intimidation or harassment; or

(c) discrimination, disadvantage or adverse treatment in relation to a person's employment, career, profession, trade or business, including the taking of disciplinary action.

2.9 Employee

For the purpose of this policy, employee is defined as any staff member who receives compensation, either full or part time, from Computershare Limited or any of its subsidiaries or related entities.

2.10 Management

For the purpose of this policy, management is defined as any administrator, manager, director, supervisor, or other individual who manages or supervises funds or other resources, including human resources.

2.11 C-Level Officer

For the purpose of this policy, C-Level Officer is defined as the Chief Executive Officer, Chief Financial Officer, Chief Technology Officer (or Executive Director – Technology) or Global Enterprise Risk and Audit Manager."

3. WHISTLEBLOWER POLICY STATEMENT

Computershare is committed to complying with the laws and regulations by which it is governed, laws and regulations that vary by jurisdiction. An integral component of this commitment is our dedication to abiding by the controls and procedures set forth in this policy – the Computershare Whistleblower Policy Incorporating Whistleblower Protection.

Computershare recognises the value of transparency and accountability in its administrative and management practices and supports the making of disclosures that reveal improper conduct or mismanagement of Computershare resources.

Computershare's internal controls and operating procedures are intended to detect and prevent improper conduct, as set out in the Computershare Code of Ethics and other prohibited behavior outlined in the Employee Handbook. However, even the best systems of control cannot guarantee absolute immunity from inappropriate workplace behavior. Computershare recognises that intentional and unintentional violations of laws, regulations, policies and procedures may occur and constitute improper conduct as defined by this policy.

Understanding this potential, Computershare is implementing an efficient and effective whistleblowing system that contains procedural requirements and guidelines. Specifically, this system addresses the reporting system, assessment of disclosures, the investigation of alleged improper activity, the management of the whistleblower (to include welfare and confidentiality) and the review process for ensuring the policy and procedures remain effective.

Computershare will not tolerate improper conduct, which generally involves violations of the Computershare Code of Ethics and other prohibited behavior outlined in the Employee Handbook. All allegations of suspected improper activity will be dealt with at a level of severity consistent with Computershare's desire to eradicate the same.

Computershare will take all reasonable steps, and do all things necessary, to protect those who make protected disclosures from any detrimental action in reprisal for the making of the disclosure. Computershare will also deal fairly with employee (s) who are the subject of the disclosure.

Computershare is committed to implementing 'best practice' policies and procedures for dealing with allegations of suspected improper activity (as defined by this policy) and the management (and protection) of the individual(s) making the allegation, and this Policy is therefore subject to review from time to time at the discretion of the Board of Directors.

The current version of the Policy will be maintained in the Global Whistleblower site.

4. REPORTING SYSTEM

A sound reporting system that instills confidence in employees and promotes trust in the integrity and effectiveness of that same system is vital to the successful design and operation of the whistleblower policy. Computershare will employ the

following mechanisms to facilitate the disclosure of suspected improper conduct:

4.1 Protected Disclosure Coordinator

The Regional Head of Risk and Audit will function as the nominated Protected Disclosure Coordinator for each major region as appointed by the Global Enterprise Risk and Audit Manager, who holds the authority to appoint and modify the Protected Disclosure Coordinator.

Disclosure of suspected improper activity or detrimental action (as defined by this policy) may be made to the relevant Protected Disclosure Coordinator appointed for Asia-Pacific, United States, Canada, Europe and South Africa. Details of the Protected Disclosure Coordinator for each of these regions are available on the Global Whistleblower site.

All correspondence (with the exception stated in s4.2 below) must be referred to the applicable Protected Disclosure Coordinator.

4.1.1 Discreet Disclosure

In the case where a person is contemplating making a disclosure but is concerned about contacting (or being seen with) the Protected Disclosure Coordinator, they can contact the Protected Disclosure Coordinator (remotely) to arrange a meeting in a discreet location usually away from the work environment.

4.2 Anonymous Disclosure

In some exceptional circumstances, the whistleblower may wish for their identity to remain unknown even to the Protected Disclosure Coordinator. In this case, the assessment and investigation of the disclosure may be more difficult without the ongoing authority and cooperation of the whistleblower; however, the allegation will still be investigated if the Protected Disclosure Coordinator believes the allegation serious enough to warrant 'anonymous investigation'.

To facilitate this, Computershare will implement the following processes:

4.2.1 Anonymous Online Disclosure

Computershare will provide, for the benefit of whistleblowers wishing to remain anonymous, the ability to make a disclosure to the Protected Disclosure Coordinator via the Global Whistleblower site. The site has been designed to ensure that the identity of the whistleblower may not be divulged to any party involved in the process. The Global Whistleblower site can be accessed through your local Computershare intranet.

4.2.2 Protected Disclosure Hotline

The relevant Protected Disclosure Coordinator's direct dial telephone line may be used by whistleblowers who wish to remain unidentified.

4.2.3 Anonymous (Registered) Mail

Computershare will take receipt of registered mail through the postal system that allows the whistleblower to remain anonymous by withholding their name and contact details. Registered mail should be sent to the Coordinator with an indication of Private and Confidential on the envelope. This mail will be delivered to the Coordinator by the Mail/Image Center unopened.

4.3 Disclosure Methods

There are many methods by which whistleblowers may make a disclosure, from a phone call to a casual chat in the lunchroom, to a written disclosure posted to the Protected Disclosure Coordinator. This section aims to provide a few

examples of the possible methods and provide assistance to whistleblowers who are unsure of how to make a disclosure.

Disclosure of suspected improper activity or detrimental action can be made through formal or informal channels:

4.3.1 Formal

There are a number of formal methods of making a disclosure, including:

Completion of the formal Protected Disclosure Document:

This is a questionnaire style document that asks questions directly related to the disclosure that the Protected Disclosure Coordinator will require. Blank copies of this document will be made available to staff at all times via the Company's intranet.

A personally written formal disclosure;

A formal meeting with the Protected Disclosure Coordinator;

Anonymous disclosure using either:

- Anonymous email address;
- Protected disclosure hotline; or
- Anonymous (registered) mail.

A phone call maintaining a sense of formality; or

A formal email.

4.3.2 Informal

There are also many informal ways to make a disclosure, which might include:

An informal meeting with the Protected Disclosure Coordinator;

A casual phone call;

Casual discussion;

Casual email; or

Any other communication chosen by the person making the disclosure.

5. DEFINING ROLES AND RESPONSIBILITIES

It is important that the roles and responsibilities of all parties associated (or potentially associated) with the whistleblowing process are clearly defined and transparent. Having clearly defined roles and responsibilities for all parties involved will reduce the potential for misunderstanding, miscommunication and mismanagement of the whistleblowing process.

5.1 All Computershare Employees

All Computershare employees are encouraged, and have the responsibility to, report any known or suspected incidences of improper activity or detrimental action in accordance with this policy.

All employees of Computershare also have an important responsibility concerning the welfare of the whistleblower within the organisation. All employees must refrain from any activity that is, or could be perceived to be, victimisation or harassment of a person who makes a disclosure. All employees must not, under any circumstance, engage in any activity that would constitute detrimental action (as defined by this policy).

All Computershare employees must take all reasonable steps to attempt to maintain the confidentiality of a person they

know or suspect to have made a disclosure.

5.2 Protected Disclosure Coordinator

The nominated Protected Disclosure Coordinator, identified regionally, is accountable for the core operation of the whistleblower policy and holds a significant burden of responsibility. The role of the Protected Disclosure Coordinator is vastly important to the success of the policy, and their responsibilities are defined to include, but not be limited to:

- Providing general advice about the operation of the whistleblower policy for any person wishing to make a disclosure about improper conduct or detrimental action;
- Acting as a point of contact for employees to field questions, provide assistance or support during the disclosure process; and more specifically:
  - Receiving all phone calls, emails and letters from employees seeking to make a disclosure;
  - Making arrangements for a disclosure to be made privately and discreetly and, if necessary, outside the work environment;
  - Receiving any disclosure made orally or in writing;
  - Committing to writing any disclosure made orally;
  - Impartially assessing the allegation and determining whether it is a disclosure made in accordance with the procedures set out in this policy; and
  - Taking all steps necessary to ensure the identity of the whistleblower and the identity of the person subject to the allegation remain confidential.

The Protected Disclosure Coordinator is also responsible for:

- Liaising with the appropriate authorities (both internal and external) usually by immediate contact with the Global Enterprise Risk and Audit Manager when a disclosure occurs, or other C-Level officer(s) as appropriate.
- After consultation with a C-Level officer, carrying out, or appointing an investigator to carry out, an investigation resulting from a disclosure;
- Overseeing and coordinating an investigation where an investigator has been appointed;
- Appointing a welfare manager to provide support to the whistleblower and to protect them from any reprisals or detrimental action resulting from making a disclosure;
- Keeping the whistleblowerand the subject of the disclosure informed as to the progress of the investigation into the disclosed matter;
- Establishing and maintaining a confidential filing system;
- Collating and publishing statistics on disclosures made; and
- Taking all necessary steps in consultation with the Global Enterprise Risk and Audit Manager to ensure the whistleblower process is fair and just.

5.3 Investigator

An internal investigator or an investigator appointed by the Protected Disclosure Coordinator in consultation with the regional Chief Legal Officer and Global Enterprise Risk and Audit Manager will be responsible for carrying out an internal investigation into the disclosure that has been made.

5.4 Welfare Manager

The Welfare Manager is responsible for the general welfare and protection of the whistleblower against reprisal and

detrimental action. The specific responsibilities of the welfare manager will include:

- Examining the immediate welfare and protection needs of a whistleblower who has made a disclosure and seek to foster a supportive work environment;
- Advising the whistleblower of the legislative and administrative protections available to them;
- Listening and responding to any concerns of harassment, intimidation or victimisation in reprisal for making a disclosure; and
- Ensuring the expectations of the whistleblower are realistic.

The welfare manager will be appointed by the Protected Disclosure Coordinator in consultation with the regional Chief Legal Officer and Global Enterprise Risk and Audit Manager on a case-by-case basis. In certain circumstances a suitably qualified Welfare Manager independent to Computershare may be appointed, with prior approval of a C-Level officer.

6. CONFIDENTIALITY

Computershare will take all reasonable steps to protect the identity of the whistleblower. Maintaining confidentiality is crucial in ensuring reprisals are not made against a whistleblower.

The Protected Disclosure Coordinator will ensure all files, whether paper or electronic, are kept in a secure room and can only be accessed as necessary by Protected Disclosure Coordinator, C-Level officers, the investigator or welfare manager (in relation to welfare matters). All printed material will be kept in files that are clearly marked as a whistleblower protection matter, and warn of the criminal penalties that apply to any unauthorised disclosure of information concerning a protected disclosure. All electronic files will be produced and stored on Protected Disclosure Coordinator's computer and given password protection. Backup files will be kept on floppy disk. All materials relevant to an investigation, such as tapes from interviews, will also be stored securely with the whistleblower files. Documents relevant to a whistleblower matter must not be shared and all phone calls and meetings must be conducted in private.

7. COLLATING AND PUBLISHING STATISTICS

The Protected Disclosure Coordinator will establish a secure register to record the information required to be published in the annual report, and to generally keep account of the status of whistleblower disclosures. The register will be confidential and will not record any information that may identify the whistleblower. The register will contain the following information:

- The number and types of disclosures made during the year;
- The number and types of disclosures referred by Computershare to an independent consultant for investigation;
- The number and types of investigations taken over from Computershare by independent investigators;
- The number of requests made by a whistleblower for the investigation to be taken over by an independent consultant;
- The number and types of disclosed matters that were declined for investigation;
- The number and types of disclosed matters that were substantiated upon investigation and the action taken on completion of the investigation; and
- Any recommendations made as a result of the investigation.

Statistics such as (but not limited to) those above will be published in a report to the board of directors on an annual basis, with a report to be produced on demand if and when the board deems necessary.

8. RECEIVING AND ASSESSING DISCLOSURES

When receiving and assessing disclosures there are a number of issues to consider.

8.1 Made in accordance with the Policy?

Where a disclosure has been received, the Protected Disclosure Coordinator will assess whether the disclosure has been made in accordance with the policies and procedures set out in this document and is, therefore, a legitimate disclosure.

8.2 Made to the appropriate person?

For the disclosure to be responded to by Computershare, it must concern an employee of Computershare. If the disclosure *does* concern an employee of Computershare, it should be made to the Protected Disclosure Coordinator.

If the disclosure concerns an employee or member of another company or public body, the person who has made the disclosure must be advised of the correct person or body to whom the disclosure should be directed. If the disclosure has been made anonymously, it should be referred to the relevant independent body.

8.3 Is it a protected disclosure?

To be a protected disclosure, a disclosure must satisfy the following criteria:

- Did a natural person (that is, an individual person rather than a corporation) make the disclosure?
- Does the disclosure relate to conduct of a Computershare employee?
- Is the alleged conduct either improper conduct or detrimental action taken against a person in reprisal for making a protected disclosure?
- Does the person making a disclosure have reasonable grounds for believing the alleged conduct has occurred?
- Is the whistleblower an employee of Computershare?

The Protected Disclosure Coordinator in consultation with the regional Chief Legal Officer and Global Enterprise Risk and Audit Manager will determine whether the disclosure is a protected disclosure. Where a disclosure is assessed not to be a protected disclosure, the matter does not need to be dealt with under the relevant legislation. The Protected Disclosure Coordinator in conjunction with the regional Chief Legal Officer and Global Enterprise Risk and Audit Manager will decide how the matter should be addressed.

9. INVESTIGATIONS

9.1 Introduction

Where assessment of the disclosure reveals the need for an investigation, the Protected Disclosure Coordinator in consultation with the regional Chief Legal Officer and Global Enterprise Risk and Audit Manager will appoint an investigator to carry out the investigation. The objectives of an investigation will be:

- To collate information relating to the allegation as quickly as possible. This may involve taking steps to protect or preserve documents, materials and equipment;
- To consider the information collected and draw conclusions objectively and impartially;
- To maintain procedural fairness in the treatment of witnesses and the person who is the subject of the disclosure;
- To protect the identify of the whistleblower; and

- To make recommendations to a C-Level officer arising from the conclusions drawn concerning remedial or other

appropriate action.

9.2 Terms of reference

Before commencing an investigation, the Protected Disclosure Coordinator will draw up terms of reference and obtain authorisation for those terms by the regional Chief Legal Officer and Global Enterprise Risk and Audit Manager, or if the matter relates to an area under the control of the regional Chief Legal Officer, by the Chief Executive Officer. The terms of reference will set a date by which the investigation report is to be concluded, and will describe the resources available to the investigator to complete the investigation within the time set. The relevant C-Level officer may approve, if reasonable, an extension of time requested by the investigator. The terms of reference will require the investigator to make regular reports to the Protected Disclosure Coordinator of general progress and such reports should be delivered to the relevant C-Level officer immediately.

9.3 Investigation plan

The investigator will prepare an investigation plan for approval by the Protected Disclosure Coordinator. The plan will list the issues to be substantiated and describe the avenue of inquiry. It will address the following issues:

- What is being alleged?
- What are the possible findings or offences?
- What are the facts in issue?
- How is the inquiry to be conducted?
- What resources are required?

At the commencement of the investigation, the whistleblower should be:

- Notified by the investigator that he or she has been appointed to conduct the investigation; and
- Asked to clarify any matters and provide any additional material he or she might have.

The investigator will be sensitive to the whistleblower's possible fear of reprisals and will be aware of the statutory protections (according to jurisdiction) provided to the whistleblower.

9.4 Natural justice

Any investigation and resulting disciplinary proceedings will be conducted by the organisation having regard to the principles of natural justice.

9.5 Conduct of the investigation

The investigator will make contemporaneous notes of all discussions and phone calls, and all interviews with witnesses will be taped. All information gathered in an investigation will be stored securely. Interviews will be conducted in private and the investigator will take all reasonable steps to protect the identity of the whistleblower. Where disclosure of the identity of the whistleblower cannot be avoided, due to the nature of the allegations, the investigator will warn the whistleblower and his or her welfare manager of this probability. It is in the discretion of the investigator to allow any witness to have legal or other representation or support during an interview. If a witness has a special need for legal representation or support, permission should be granted.

9.6 Reporting requirements

The Protected Disclosure Coordinator will ensure the whistleblower is kept regularly informed concerning the handling of a protected disclosure and an investigation. The Protected Disclosure Coordinator will report to the appropriate officers of

Computershare (such as the board of directors or a C-Level officer) about the progress of the investigation.

If the whistleblower requests information about the progress of an investigation, that information will be provided within 28 days of the date of the request.

10. ACTION TAKEN AFTER AN INVESTIGATION

10.1 Investigator's Final Report

At the conclusion of the investigation, the investigator will submit a written report of his or her findings to the Protected Disclosure Coordinator. The report will contain:

- The allegation/s;
- An account of all relevant information received and, if the investigator has rejected evidence as being unreliable, the reasons for this opinion being formed;
- The conclusions reached and the basis for them; and
- Any recommendations arising from the conclusions.

If the investigator has found that the conduct disclosed by the whistleblower has occurred, recommendations made by the investigator will include:

- The steps that need to be taken by Computershare to prevent the conduct from continuing or occurring in the future; and
- Any action that should be taken by Computershare to remedy any harm or loss arising from the conduct. This action may include bringing disciplinary proceedings against the person(s) responsible for the conduct, and referring the matter to an appropriate authority for further consideration.

The report will be accompanied by:

- The transcript or other record of any oral evidence taken, including tape recordings; and
- All documents, statements or other exhibits received by the investigator and accepted as evidence during the course of the investigation.

Where the investigator's report is to include an adverse comment against any person, that person will be given the opportunity to respond and his or her defense will be fairly included in the report.

The report will not disclose particulars likely to lead to the identification of the whistleblower.

10.2 Action to be taken

If the Protected Disclosure Coordinator is satisfied that the investigation has found that the disclosed conduct has occurred, he or she will recommend the action that must be taken to prevent the conduct from continuing or occurring in the future. The Protected Disclosure Coordinator may also recommend that action be taken to remedy any harm or loss arising from the conduct.

The Protected Disclosure Coordinator will provide a written report to the board of directors, the Global Enterprise Risk and Audit Manager and the whistleblower setting out the findings of the investigation and any remedial steps taken.

Where the investigation concludes that the disclosed conduct did not occur, the Protected Disclosure Coordinator will report these findings to the Global Enterprise Risk and Audit Manager and to the whistleblower.

11. MANAGING THE WELFARE OF THE WHISTLEBLOWER

11.1 Commitment to protecting whistleblowers

Computershare is committed to the protection of genuine whistleblowers against detrimental action taken in reprisal for the making of protected disclosures. The Protected Disclosure Coordinator is responsible for ensuring whistleblowers are protected from direct and indirect detrimental action, and that the culture of the workplace is supportive of protected disclosures being made.

The Protected Disclosure Coordinator will appoint a welfare manager to all whistleblowers who have made a protected disclosure. The welfare manager will:

- Examine the immediate welfare and protection needs of a whistleblower who has made a disclosure andseek to foster a supportive work environment;
- Advise the whistleblower of the legislative and administrative protections available to him or her;
- Listen and respond to any concerns of harassment, intimidation or victimisation in reprisal for making disclosure;
- Keep a contemporaneous record of all aspects of the case management of the whistleblower including all contact and follow-up action; and
- Ensure the expectations of the whistleblower are realistic.

All employees will be advised that it may be an offence for a person to take detrimental action in reprisal for a protected disclosure. Depending on the laws in each jurisdiction, the penalty may be a fine or imprisonment or both. The taking of detrimental action in breach of this provision can also be grounds for making a disclosure under the policy and can result in an investigation. The person taking detrimental action may be subject to disciplinary action by the company, up to and including termination.

Detrimental action includes:

- Causing injury, loss or damage;
- Intimidation or harassment; and
- Discrimination, disadvantage or adverse treatment in relation to a person's employment, career, profession, trade or business (including the taking of disciplinary action).

11.2 Keeping the whistleblower informed

The Protected Disclosure Coordinator will ensure the whistleblower is kept informed of action taken in relation to his or her disclosure, and the time frames that apply. The whistleblower will be informed of the objectives of an investigation, the findings of an investigation, and the steps taken by Computershare to address any improper conduct that has been found to have occurred. The whistleblower will be given reasons for decisions made by Computershare in relation to a protected disclosure. All communication with the whistleblower will be in plain English.

11.3 Occurrence of detrimental action

If a whistleblower reports an incident of harassment, discrimination or adverse treatment that would amount to detrimental action taken in reprisal for the making of the disclosure, the welfare manager will:

Record details of the incident;

Advise the whistleblower of his or her rights under the relevant legislation; and

Advise the Protected Disclosure Coordinator and the C-Level officer of the detrimental action.

The taking of detrimental action in reprisal for the making of a disclosure can be an offence as well as grounds for making a further disclosure. Where such detrimental action is reported, the Protected Disclosure Coordinator will assess the report as a new disclosure.

11.4 Whistleblowers implicated in improper conduct

If a person who makes a disclosure is implicated in misconduct, Computershare will handle the disclosure and protect the whistleblower from reprisals in accordance with the relevant legislation and these procedures. Computershare acknowledges that the act of whistleblowing should not shield whistleblowers from the reasonable consequences flowing from any involvement in improper conduct. A person's liability for his or her own conduct is not affected by the person's disclosure of that conduct. However, in some circumstances, an admission may be a mitigating factor when considering disciplinary or other action.

The regional Chief Legal Officer along with the Global Enterprise Risk and Audit Manager will make the final decision on the advice of the Protected Disclosure Coordinator as to whether disciplinary or other action will be taken against a whistleblower. Where disciplinary or other action relates to conduct that is the subject of the whistleblower's disclosure, the disciplinary or other action will only be taken after the disclosed matter has been appropriately dealt with. In all cases where disciplinary or other action is being contemplated, the regional Chief Legal Officer must be satisfied that it has been clearly demonstrated that:

- The intention to proceed with disciplinary action is not causally connected to the making of the disclosure (as opposed to the content of the disclosure or other available information);
- There are good and sufficient grounds that would fully justify action against any non-whistleblower in the same circumstances; and
- There are good and sufficient grounds that justify exercising any discretion to institute disciplinary or other action.

The Protected Disclosure Coordinator will thoroughly document the process including recording the reasons why the disciplinary or other action is being taken, and the reasons why the action is not in retribution for the making of the disclosure. The Protected Disclosure Coordinator will clearly advise the whistleblower of the proposed action to be taken, and of any mitigating factors that have been taken into account.

12. MANAGEMENT OF THE PERSON AGAINST WHOM THE DISCLOSURE HAS BEEN MADE

Computershare recognises that employees against whom disclosures are made must also be supported during the handling and investigation of disclosures. Computershare will take all reasonable steps to ensure the confidentiality of the person who is the subject of the disclosure during the assessment and investigation process. Where investigations do not substantiate disclosures, the fact that the investigation has been carried out, the results of the investigation, and the identity of the person who is the subject of the disclosure will remain confidential.

The Protected Disclosure Coordinator will ensure the person who is the subject of any disclosure investigated by or on behalf of Computershare is:

- Informed as to the substance of the allegations;
- Given the opportunity to answer the allegations before a final decision is made;
- Informed as to the substance of any adverse comment that may be included in any report arising from the investigation; and has
- His or her defense set out fairly in any report.

If the allegations in a disclosure have been investigated, and the person who is the subject of the disclosure is aware of the allegations or the fact of the investigation, the Protected Disclosure Coordinator will formally advise the person who is the subject of the disclosure of the outcome of the investigation.

Computershare will give its full support to a person who is the subject of a disclosure where the allegations contained in a disclosure are clearly wrong or unsubstantiated. If the matter has been publicly disclosed, the regional Chief Legal Officer and Global Enterprise Risk and Audit Manager of Computershare will consider any request by that person to issue a statement of support setting out that the allegations were clearly wrong or unsubstantiated.

13. REVIEW

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