Sektor Group Limited
525 Great South Road, Penrose
PO Box 12405, Penrose
Auckland 1642
Ph: 09 579 9855
www.sektor.co.nz

Whistleblower Policy

1. Whistleblower Policy

1.1 This Whistleblower Policy ('Policy') relates to Sektor Group Ltd, Sektor Pty Ltd, Sektor Ltd, Sektor Distributors Sdn., Bhd., and Sektor Distributors (Thailand) Co., Ltd., ('Sektor') and, where relevant, operates in conjunction with other policies relating to minimum standards of behaviour and conduct, the Contract of Employment or Contract for Services.

1.2 The Board of Directors of Sektor Group Ltd has resolved that this Policy will apply to all entities within the Sektor group of companies. Specific country policies are;

1.2.1 Australia's required whistleblower policy is under the *Australian Corporations Act 2001* (Cth);

1.2.2 New Zealand has the Protected Disclosures Act 2000 for protection of Whistleblowers.

1.2.3 Malaysia has the Whistleblower Protection Act, 2010, 711.

1.2.4 Thailand has partial protection for Whistleblowers under the Executive Measure in Anti-Corruption Act, B.E. 2551 and the penalty in Witness protection Act, B.E. 2546.

1.3 This Policy is available on the Sektor's Intranet and website.

2. Purpose

2.1 Sektor's Code of Conduct recognises the importance of a work environment which actively promotes best practice. The Code describes the standards of behaviour and conduct expected from workplace participants in their dealings with customers, suppliers, clients, co-workers, management and the general public

2.2 This Policy supplements the Code of Conduct by setting out Sektor's policy on whistleblowing and its commitment to protect whistleblowers. This whistleblower policy describes how that commitment is implemented.

2.3 The purpose of the policy includes:

a) to encourage more disclosures of wrongdoing;

b) to help deter wrongdoing, in line with Sektor's risk management and governance framework;

c) to ensure individuals who disclose wrongdoing can do so safely, securely and with confidence that they will be protected and supported;

d) to ensure disclosures are dealt with appropriately and on a timely basis;

e) to provide transparency around Sektor's framework for receiving, handling and investigating disclosures;

f) to support Sektor's values and code of conduct;

g) to support Sektor's long-term sustainability and reputation; and

h) to meet Sektor's legal and regulatory obligations.

3. Who does this policy apply to?

3.1 Sektor is committed to making this Policy available for concerns affecting Sektor's activities held by:

a) current or former employees and officers of Sektor, whether full-time, part-time or casual, at any level of seniority and wherever employed;

b) a person who has or had a contract to supply services or goods, to Sektor;

c) a current or former employee of a person who has or had a contract to supply services or goods to Sektor;

d) a current or former associate of Sektor (eg a director of Sektor); and

e) a current or former relative, spouse or dependent of any of the above.

4. What is Reportable Conduct?

4.1 Reportable Conduct is information that the discloser has reasonable grounds to suspect concerns misconduct or an improper state of affairs or circumstances in relation to Sektor. Reportable Conduct includes the following types of wrongdoing:

a) conduct or practices which are illegal or breach any law or regulation, or significantly breach any contract binding a member of Sektor;

b) fraudulent or corrupt practices (including offering or accepting bribes or otherwise gaining advantage from a relationship with Sektor to which Sektor has not agreed);

c) a serious breach, or continuing or regular breaches of Sektor's policies or other rules of conduct;

d) coercion, harassment or discrimination by, or affecting, any member of Sektor's team members;

e) misleading or deceptive conduct of any kind;

f) situations within Sektor's control that pose a danger to the health or safety of any person; and

g) situations within Sektor 's control that are a significant danger to the environment.

4.2 Personal workplace-related grievances are not covered under the scope of this policy (unless such grievance is in relation to victimisation as a result of making a disclosure under this Policy). Examples of personal work-related grievances include disclosures regarding interpersonal conflicts with other employees, transfer and promotion decisions, decisions regarding the terms and conditions of employment, decisions regarding suspension and termination of employment and disciplinary decisions.

5. Who can receive a disclosure of Reportable Conduct?

5.1 If you become aware, on reasonable grounds, of any issue or behaviour that amounts to Reportable Conduct and you wish to report your concerns, then you must report that concern to an Eligible Recipient.

5.2 An Eligible Recipient is:

a) an Officer or senior manager. An Officer includes a director or company secretary of Sektor;

b) the Whistleblower Protection Officer (WPO) with authority to receive protected disclosures;

c) Sektor's Auditor;

d) a legal practitioner for the purpose of obtaining legal advice or legal representation in relation to the operation of this Policy;

e) the authorities responsible for the enforcement of the law in the relevant area; or

f) email your concerns to legal@sektor.co

5.3 A Whistleblower Protection Officer is a senior manager of Sektor, designated, authorised and trained to receive whistleblower disclosures. If you wish to report Reportable Conduct, Sektor encourages you to report your concerns to our designated WPO because of their familiarity with this policy. However, if you would prefer you may report your concerns to any other Eligible Recipient or directly to legal@sektor.co.

5.4 An Eligible Recipient who is not a WPO is required to notify the WPO or email legal@sektor.co of the report within 2 business days. If the Reportable Conduct concerns the WPO, the Eligible Recipient must notify the CEO or legal@sektor.co of the report.

5.5 The contact details for Sektor's designated WPO is set out in clause 16.

6. Public Interest Disclosures and Emergency Disclosures

6.1 Protection will only be offered by Sektor to any discloser who informs a Member of Parliament or journalist of concerns about Reportable Conduct if the disclosure falls within the Public Interest Disclosure and Emergency Disclosure criteria below.

Public Interest Disclosure

6.2 To receive 'Public Interest Disclosure' protection under this Policy, the discloser must satisfy the following:

a) The discloser has previously made a report regarding the Reportable Conduct to an Eligible Recipient; and

b) At least 90 days have passed since the report was made; and

c) The discloser does not have reasonable grounds to believe that action is being, or has been taken to address the report; and

d) The discloser has reasonable grounds to believe that making a further report would be in the public interest; and

e) After 90 days have passed since the disclosure, the discloser provides written notification to Sektor's Chair, CEO or WPO that:

i) includes sufficient information to identify the previously made report; and

ii) clearly states that the discloser intends to make a public interest disclosure; and

f) The information disclosed is no greater than necessary to inform the Member of Parliament or journalist of the misconduct or the otherwise improper state of affairs.

Emergency Disclosure

6.3 A discloser will be offered protection under this Policy for 'Emergency Disclosure' if the following criteria are satisfied:

a) The discloser has previously reported the Reportable Conduct to an Eligible Recipient; and

b) The discloser has reasonable grounds to believe that the information concerns a substantial and imminent danger to the health and safety of a person, persons, or the environment; and

c) The discloser provides the Eligible Recipient with written notification of the Reportable Conduct which includes sufficient information to identify the previous disclosure and states the discloser intends to make an emergency disclosure; and

d) The emergency disclosure is made to a Member of Parliament or a journalist; and

e) The information disclosed is no greater than necessary to inform the Member of Parliament or journalist of the misconduct or the otherwise improper state of affairs.

7. How to make a disclosure of Reportable Conduct?

7.1 To make a disclosure of Reportable Conduct, at the very least, you need to be able to tell the Eligible Recipient whom you reasonably suspect is involved in the misconduct, when it occurred and who is affected.

7.2 Sektor encourages you to make disclosures of Reportable Conduct in writing including by email but disclosures can also be made over the phone.

7.3 The more evidence you provide to the Eligible Recipient, the more effective the investigation is likely to be. However, you should not delay approaching the Eligible Recipient once you have reasonable grounds to suspect Reportable Conduct.

8. Can disclosures be made anonymously?

8.1 Disclosure may be anonymous and the protections under this Policy will apply even if you do not give your name. However, it may assist in the investigation process if the name of the discloser is provided to the Eligible Recipient. If you choose to disclose your name, this is done so on a strictly confidential basis.

9. Legal protections for disclosers

9.1 The legal protections for disclosers under this Policy include.

a) identity protection;

b) protection form detrimental acts or omissions;

c) compensation and other remedies; and

d) civil, criminal and administrative liability protection.

Identity protection

9.2 The identity of a discloser or information that is likely to lead to the identification of the discloser cannot be disclosed except:

a) within Australia, to ASIC, APRA, or a member of the Australian Federal Police (within the meaning of the *Australian Federal Police Act 1979*) or to the relevant authorities outside of Australia in accordance with local laws;

b) to a legal practitioner (for the purposes of obtaining legal advice or legal representation about the whistleblower provisions in the Corporations Act);

c) to a person or body prescribed by regulations; or

d) with the consent of the discloser.

Outside of Australia local laws may contain other exceptions.

9.3 If anyone discloses your identity in breach of clause 9.2 you can lodge a complaint with the WPO whose details are set out in clause 16. In Australia, you can also lodge a complaint with a regulator such as ASIC for investigation.

Protection from detrimental acts or omissions

9.4 A person cannot engage in conduct that causes detriment to a discloser (or another person), in relation to a disclosure, if:

a) the person believes or suspects that the discloser (or another person) made, may have made, proposes to make or could make a disclosure that qualifies for protection; and

b) the belief or suspicion is the reason, or part of the reason, for the conduct.

9.5 In addition, a person cannot make a threat to cause detriment to a discloser (or another person) in relation to a disclosure.

9.6 Detrimental conduct includes:

a) dismissal of an employee;

b) injury of an employee in his or her employment;

c) alteration of an employee's position or duties to his or her disadvantage;

d) discrimination between an employee and other employees of the same employer;

e) harassment or intimidation of a person;

f) harm or injury to a person, including psychological harm;

g) damage to a person's property;

h) damage to a person's reputation; or

i) damage to a person's business or financial position.

9.7 Detrimental conduct does not include:

a) administrative action that is reasonable for the purpose of protecting a discloser from detriment (e.g. moving a discloser who has made a disclosure about their immediate work area to another office to prevent them from detriment); or

b) managing a discloser's unsatisfactory work performance, if the action is in line with Sektor's performance management framework

Compensation and other remedies

9.8 A discloser (or any other employee or person) can seek compensation and other remedies through the courts if:

a) they suffer loss, damage or injury because of a disclosure; and

b) Sektor failed to take reasonable precautions and exercise due diligence to prevent the detrimental conduct.

9.9 You should seek independent legal advice before seeking compensation or other remedies through the courts.

Civil, criminal and administrative liability protection

9.10 A discloser is protected from any of the following in relation to their disclosure:

a) civil liability (e.g. any legal action against the discloser for breach of an employment contract, duty of confidentiality or another contractual obligation);

b) criminal liability (e.g. attempted prosecution of the discloser for unlawfully releasing information, or other use of the disclosure against the discloser in a prosecution (other than for making a false disclosure)); and

c) administrative liability (e.g. disciplinary action for making the disclosure).

9.11 These protections do not grant immunity for any misconduct a discloser has engaged in that is revealed in their disclosure.

10. Support and practical protection for disclosers

10.1 Sektor will take the following steps to support disclosers and protect disclosers from detriment.

Identity protection (confidentiality)

10.2 To reduce the risk that a discloser will be identified from the information contained in a disclosure, Sektor will:

a) redact all personal information or reference to the discloser witnessing an event;

b) refer to the discloser in a gender-neutral context;

c) where possible, contact the discloser to identify aspects of their disclosure that could inadvertently identify them; and

d) ensure that disclosures are handled and investigated by qualified staff.

10.3 To keep information contained in a disclosure secure, Sektor will ensure that:

a) all paper and electronic documents and other materials relating to disclosures will be stored securely;

b) access to all information relating to a disclosure will be limited to those directly involved in managing and investigating the disclosure;

c) only a restricted number of people who are directly involved in handling and investigating a disclosure will be made aware of a discloser's identity (subject to the discloser's consent) or information that is likely to lead to the identification of the discloser;

d) communications and documents relating to the investigation of a disclosure will not to be sent to an email address or to a printer that can be accessed by other staff; and

e) each person who is involved in handling and investigating a disclosure will be reminded about the confidentiality requirements, including that an unauthorised disclosure of a discloser's identity may be a criminal offence:

Protection from detrimental acts or omissions

10.4 To protect a discloser from detrimental acts or omissions, Sektor will:

a) assess the risk of detriment against a discloser and other persons (e.g. other staff who might be suspected to have made a disclosure), as soon as practicable after receiving a disclosure;

b) assess the risk of detriment against a discloser and other persons (e.g. other staff who might be suspected to have made a disclosure), as soon as practicable after receiving a disclosure;

c) develop strategies to help a discloser minimise and manage stress, time or performance impacts, or other challenges resulting from the disclosure or its investigation;

d) where practicable, allow the discloser to perform their duties from another location, reassign the discloser to another role at the same level, make other modifications to the discloser's workplace or the way they perform their work duties, or reassign or relocate other staff involved in the disclosable matter;

e) ensure that management are aware of their responsibilities to maintain the confidentiality of a disclosure, address the risks of isolation or harassment, manage conflicts, and ensure fairness when managing the performance of, or taking other management action relating to, a discloser;

f) intervene to protect a discloser if detriment has already occurred.

10.5 Sektor's Employee Assistance program is available to any employees who need support, guidance or counselling 24/7.

11. Handling a disclosure

11.1 On receiving a disclosure to which this Policy may apply, a WPO will assess each disclosure to determine whether:

a) it qualifies for protection; and

b) a formal, in-depth investigation is required.

12. Investigating a disclosure

12.1 If the WPO assesses that an investigation is required, the WPO will determine the form of the investigation depending on the nature of the disclosure.

12.2 Investigations may be conducted by internally or referred to an independent investigator depending on the complexity and subject matter of the disclosure.

12.3 Without the discloser's consent Sektor will not disclose information that is likely to lead to the identification of the discloser as part of the investigation process. This may impact the effectiveness of the investigation.

12.4 All investigations will:

a) maintain the confidentiality of all parties, including witnesses;

b) apply procedural fairness to all parties;

c) maintain strict security;

d) ensure that all information obtained is properly secured to prevent unauthorised access;

e) ensure that all relevant witnesses are interviewed and documents examined; and

f) ensure that contemporaneous notes of all discussions, phone calls and interviews are made.

12.5 When the WPO has determined the nature of the investigation, the WPO will advise the discloser including the time frame for the investigation. The WPO will also provide the discloser with regular updates on the conduct of the investigation.

12.6 The findings of the investigation must be in writing and must include:

a) a description of the allegations;

b) a statement of all relevant findings of fact and the evidence relied upon to reach conclusions on each allegation;

c) the basis for each conclusion reached (including the damage caused, if any, and the impact on the organisation and other affected parties);

d) recommendations based on those conclusions to address any wrongdoing identified and any other matters arising during the investigation.

12.7 The findings will be provided to the WPO who will review the findings and make recommendations to the CEO and/or the Chair for review. If the investigation concerns both the CEO and the Chair, the WPO will make recommendations to the chair of Sektor's Board's [Audit and Risk Committee] or another director.

13. Availability

13.1 This Policy will be available on Sektor's intranet and the website.

14. Review of the whistleblowing program and this policy

14.1 The whistleblowing program (including this Policy) is reviewed regularly by the Board through the [Audit and Risk Committee]. A report summarising this review and proposing recommendations is made to the Board. The review must address generally the efficacy of the whistleblowing program, in particular:

a) the fairness of investigations undertaken;

b) the actual consequences of making disclosures;

c) the performance of the WPO; and

d) compliance with this policy.

15. Breaches of this Policy

15.1 A breach of this Policy may lead to disciplinary action including, but not limited to, termination of employment or services.

16. Whistleblower Protection Officer

16.1 Sektor's Whistleblower Protection Officer is Michael Bryan mikeb@sektor.co.nz

Variations

Sektor reserves the right to vary or replace this Policy from time to time.

Policy version and revision information

Policy authorised by: Board Of Directors, Sektor Group Ltd. Date of review: Apr 2024