Sample Whistleblower Policy

September 2020

Notice

This sample whistleblower Policy is based on observations of selected companies and the requirements of CSA National Instrument 52-110, *Audit Committees*.

Table of contents

1.0 Objective

1.1 The Organization expects each director, officer, employee, and contractor to comply with all applicable laws and stock exchange requirements. The Organization is committed to promoting honesty and integrity and maintaining the highest ethical standards in all its activities. Consistent with these values, the Organization does not tolerate any illegal or unethical behaviour, including fraud, criminal acts, regulatory violations, manipulation of accounting and auditing records, or any breach of the Code (defined below) or any other policies, procedures, or practices established by the Organization (and its subsidiaries and affiliates, as applicable).

1.2 The Audit Committee must ensure the Organization has the appropriate procedures for (i) the receipt, retention, and treatment of Incidents (defined below), and (ii) the confidential, anonymous reporting of concerns regarding questionable accounting or auditing matters. This Policy serves to fulfill these Audit Committee responsibilities.

2.0 Definitions

2.1 **"Administrator"** means the person designated by the board to oversee the day- to-day administration of this Policy, including receiving, tracking, and reporting to the board on Incidents reported.

2.2 **"Audit Committee"** means the audit committee appointed by the Organization's board of directors;

2.3 **"Board"** means the Organization's board of directors;

2.4 **"Code"** means the Code of Conduct adopted by the Board and, if applicable, any similar Policy adopted by the board of directors of any Organization subsidiary or affiliate;

2.5 **"Organization"** means (Legal name of the Organization);

2.6 **"Employee Reporter"** means an Organization's employee or contractor reporting Incidents under this Policy;

2.7 **"Incident"** means one or more violations or suspected violations of the Code, applicable laws, or the Organization's accounting, financial reporting, internal accounting controls, or auditing policies and procedures, or related matters, including, but not limited to, the following non-exhaustive list of examples:

2.7.1 suspected violations of applicable law, whether civil or criminal, including breaches of occupational health and safety legislation;

2.7.2 suspected violations of corporate policies or guidelines of the Organization or the Code;

2.7.3 questionable accounting, internal accounting controls, auditing practices or accounting or auditing irregularities;

2.7.4 experiencing or observing discrimination, harassment, sexual misconduct, workplace violence, substance abuse, violations of human rights, or similar behaviours;

2.7.5 any falsification of contracts, books, records, reports, or accounts;

2.7.6 direct or indirect participation in any bribes, kickbacks, improper profit-sharing arrangements, illegal gratuities or improper inducements or payments to any public official or other acts of corruption or bribery;

2.7.7 fraud against or involving the Organization, its subsidiaries or affiliates or any party having a business relationship with the Organization or its subsidiaries or affiliates;

2.7.8 risks to the Organization's assets, property, or resources;

2.7.9 risks to the environment;

2.7.10 any matter that involves a significant threat to the health and safety of the Organization's personnel, other representatives or business partners and/or the general public, including unsafe working conditions;

2.7.11 concerns about the Organization's business practices;

2.7.12 a matter likely to receive negative media or public attention; or

2.7.13 any retaliation against any Reporter for intending to make or making a good faith report under this Policy.

2.8 **"Investigator"** means the person or persons designated by the board with responsibility for investigating and bringing closure to reported Incidents;

2.9 **"Policy"** means this *Whistleblower Policy*; and

2.10 **"Reporter"** means an Employee Reporter or a director, officer or other person reporting Incidents in accordance with this Policy, including but not limited to suppliers, business partners, consultants, agents and representatives.

3.0 Application

3.1 This Policy applies to each Incident reported, and the procedures, protections and other provisions of this Policy are for the benefit of every director, officer, employee, and contractor of the Organization and of each Organization subsidiary that has not adopted a substantially similar Policy.

3.2 The Administrator shall serve as the main Organization contact for subsidiaries in relation to the administration of equivalent subsidiary policies and shall oversee reporting to the Audit Committee regarding such matters.

4.0 No retaliation

4.1 The Organization will not, in relation to the reporting of any Incident under the Policy, permit any form of retaliation or reprisal (including discharge, demotion, transfer, suspension, threat, intimidation, harassment or any other form of discrimination) by any person or group, directly or indirectly, against any Reporter, witness or interviewee who, truthfully and in good faith:

4.1.1 reports an Incident in accordance with this Policy;

4.1.2 lawfully provides information or assistance in an investigation regarding any conduct which the Reporter reasonably believes constitutes a violation of applicable laws, the Code or any other Organization policies;

4.1.3 files, causes to be filed, testifies, participates in or otherwise assists in a proceeding related to a violation of applicable laws, the Code or any other Organization policies;

4.1.4 provides a law enforcement officer with information regarding the commission or possible commission of an offence, unless the individual reporting is one of the violators; or

4.1.5 assists the Investigator, the Audit Committee, management or any other person or group (including any governmental or regulatory authority) in the investigation of an Incident.

4.2 Any director, officer, employee or contractor who retaliates against a Reporter, witness or interviewee in violation of Section 4.1 could face disciplinary action, up to and including termination of the person's employment or position with the Organization.

4.3 If any person believes that retaliation or reprisal has occurred, that person may submit a complaint pursuant to this Policy after the person knew or ought to have known that the retaliation or reprisal occurred.

5.0 Reporting incidents

5.1 Incidents must be reported promptly by Reporters to someone who can address them properly. In most cases involving an Employee Reporter, this will be the employee's supervisor.

5.2 If an Employee Reporter believes that in the circumstances it would not be appropriate to report an Incident to their supervisor, the Employee Reporter may report the Incident to any officer or other member of the Organization's management team to whom the person believes it would be appropriate to report the Incident.

5.3 Where a supervisor or other member of management receives an Incident report, it must be promptly forwarded to the Administrator.

5.4 Suspected fraud or violations of applicable laws should be promptly reported directly to the Administrator.

5.5 Reporters may report their concerns under the Policy through several channels. They should choose the channel that is most appropriate given the nature of their concern.

5.5.1 to the Administrator;

5.5.2 to the Chair of the Audit Committee; or

5.5.3 to a third-party provider of confidential, anonymous reporting services, via the internet or by telephone. The Organization has established a mechanism for confidential and anonymous submission of concerns through an independent third party, [Provider]. [Provider] provides a website ([URL]) and hotline that is accessible in all locations in which the Organization operates

24 hours a day, 7 days a week. Individuals calling the hotline from Canada or the United States can call [Phone number]. A list of telephone numbers on a worldwide basis is available at [URL].

If a report is submitted anonymously, the identity of the individual raising the concern (the Reporter) through the hotline is not known to the Organization. The Reporter will be provided with a confidential PIN number that will allow for further anonymous communication through the hotline.

Concerns raised through the hotline are submitted to the Chair of the Audit Committee and/or the CLO to ensure independent review, investigation, and disposition.

5.5.4 To external reporting channels. Certain securities commissions and other regulatory bodies may have channels through which Reporters may report their concerns. Information on such programs, including how to participate, is publicly available on relevant websites.

Important Note: The Organization takes all concerns seriously and will investigate all credible complaints. The third-party provider hotline allows the Reporter to provide additional information required by the investigations on an anonymous basis. However, employees should be aware that reporting anonymously through other channels can limit the ability of the Organization to thoroughly investigate a report if insufficient information is provided.

5.6 Access to Incident reports is strictly controlled to prevent interference with, and ensure the independence, effectiveness, and integrity of any ensuing Incident investigation. Upon receiving an Incident report, the Administrator will forward it to the Chair of the Audit Committee and the Organization's Chief Legal Officer (“CLO”) (provided such individuals are not related to or the subject of the Incident). Incident reports received through third-party provider of confidential, anonymous reporting services are automatically forwarded to the Administrator, Chair of the Audit Committee and/or CLO.

5.7 Where other Organization policies contain their own specialized reporting procedures, those other procedures should be used whenever possible instead of the reporting procedures herein.

6.0 Investigation and oversight

6.1 The Administrator has been designated by the Board and will serve as the Investigator for Incidents of a general nature that are not more appropriately investigated by another person. Where an Incident pertains to a matter more appropriately investigated by another person, the Administrator will consult with the Chair of the Audit Committee and CLO to assign an appropriate internal or external Investigator to investigate the Incident. No person will be appointed to investigate an Incident where that person is or could reasonably be perceived to be in a conflict of interest, or otherwise not impartial or unbiased in conducting the investigation.

6.2 The Investigator will investigate Incidents in an independent, expeditious, and confidential manner, taking care to protect the identity of the persons involved (in accordance with Section 8.0 below) and to ensure that the investigation is not impaired in any manner.

6.3 The Investigator will contact the Reporter to acknowledge receipt of the Incident report within [x] business days.

6.4 A Reporter who reports an Incident through a third-party provider of confidential, anonymous reporting services will be assigned a unique case identifier and password and should return to the provider website once [x] business days have elapsed after reporting an Incident to assess the response to the report and to answer anonymously any follow-up questions.

6.5 All Incidents will be promptly investigated, and appropriate corrective action will be taken if warranted by the investigation.

6.6 All persons (including the Reporter) must fully cooperate in the Investigator's investigation.

6.7 The Investigator may involve other persons in the investigation as deemed appropriate (including members of the Organization's management). The Investigator may agree to authorize an independent investigation and/or to engage external consultants to assist in the investigation. The Investigator has direct access to the Chair of the Audit Committee.

6.8 The Audit Committee shall oversee the activities of the Administrator and Investigator(s) and the investigation and resolution of Incidents. All material Incidents, including all Incidents relating to accounting, internal accounting controls, or auditing matters, will be promptly reported by the Administrator to the Chair of the Audit Committee for investigation in cooperation with and under the supervision of the Audit Committee. The Administrator will report to the Audit Committee on all other material Incidents once per quarter. The Administrator may periodically report to the Audit Committee a summary of any other non-material Incidents.

6.9 The status, and to the extent possible the outcome, of an Incident investigation will be communicated to the Reporter in a timely manner either through direct communication, if the Reporter provided his or her name, or via third-party provider of confidential, anonymous reporting services if the Reporter wishes to remain anonymous. Responses to anonymous reports made via telephone may be accessed through the provider website using the unique case identifier and password provided to the Reporter upon reporting the Incident.

7.0 Acting in good faith

7.1 A Reporter must act in good faith and have reasonable grounds for believing that the information disclosed is true.

7.2 Incidents found to have been made in bad faith, maliciously, or which were known to be false when made, will be viewed as a serious offence that could give rise to disciplinary action, up to and including termination of employment with the Organization.

8.0 Confidentiality and anonymity

8.1 All Incident reports will be treated as confidential, and each report and the identity of the Reporter will be kept confidential to the extent permissible by law and feasible to permit proper investigation and resolution. Reports will only be accessible to people that the Investigator determines have a “need to know” and where such access will not otherwise compromise or interfere with the independence, effectiveness, and integrity of the investigation. Ordinarily, a need to know arises from an obligation to investigate or to take remedial action based on the information contained in the Incident report. For

clarity, sharing Incident information in a manner required by this Policy will not be considered a breach of confidentiality.

8.2 Reports of Incidents must be supported by sufficient information and evidence to enable a proper investigation, particularly in the case of anonymous Incident reports, since the Investigator may not be able to seek further details from the Reporter. Incident reports should include:

8.2.1 the date(s) of the Incident(s);

8.2.2 the identity of individuals and witnesses involved;

8.2.3 a description of the specific actions or omissions that constitute the Incident;

8.2.4 how the Reporter became aware of the Incident;

8.2.5 any steps taken by the Reporter to date with respect to the Incident; and

8.2.6 any materials or documents relevant to support or evidence the Incident.

8.3 While this Policy facilitates anonymous reporting and protects Reporter anonymity, such measures may hinder the effective investigation of an Incident. Also, as a practical matter, it is possible that the identity of an anonymous Reporter may become known during the Incident investigation or resolution or may be subject to legal disclosure requirements. Therefore, the Organization encourages Reporters to only report anonymously where necessary, given the inherent difficulty in properly investigating, following up on, and resolving anonymously reported Incidents. If a Reporter remains anonymous and does not provide sufficient detail regarding the Incident (as per Section 8.2), the Investigator may not be able to initiate or complete a comprehensive Incident investigation.

9.0 Retention of records

9.1 Records pertaining to an Incident are the property of the Organization and shall be retained: (i) in compliance with applicable laws and the Organization's record retention policies; (ii) subject to safeguards that ensure their confidentiality and, when applicable, the anonymity of the Reporter; and (iii) in such a manner as to maximize their usefulness to the Organization's overall compliance program.

10.0 Policy review

10.1 This Policy shall be reviewed annually along with updates to the Code.

11.0 Questions

11.1 Any questions concerning this Policy should be directed to the CLO.

https://www.iasplus.com/en-ca

About Deloitte

Deloitte provides audit and assurance, consulting, financial advisory, risk advisory, tax, and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and service to address clients' most complex business challenges. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Our global Purpose is making an impact that matters. At Deloitte Canada, that translates into building a better future by accelerating and expanding access to knowledge. We believe we can achieve this Purpose by living our shared values to lead the way, serve with integrity, take care of each other, foster inclusion, and collaborate for measurable impact.

To learn more about how Deloitte's approximately 312,000 professionals, over 12,000 of whom are part of the Canadian firm, please connect with us on LinkedIn, Twitter, Instagram, or Facebook.