

**WHISTLEBLOWER POLICY****SCOPE:**

1. This policy outlines the procedure for managing misconduct, or an improper state of affairs or circumstances, relating to Device Technologies Group and each of its related entities in Australia, including:
  - 1.1 Who can make the report
  - 1.2 What is the Disclosable matter
  - 1.3 How to report a Disclosable matter
  - 1.4 The investigation process
  - 1.5 Protection provided to you if you make a report and
  - 1.6 Ensuring fair treatment of individuals mentioned in a report
2. The regulation around whistleblowing for jurisdictions outside of Australia in which Device Technologies Group operates are included in Appendix A to this policy. Without limiting local jurisdictional legal requirements, Device Technologies Group will employ best efforts to manage Disclosable Matters raised in jurisdictions outside Australia with the same intent as described in this Policy.

**1. GENERAL:****1.1. Need for this Policy**

- 1.1.1. We are committed to a culture of integrity, transparency and accountability.
- 1.1.2. We encourage you to report a Disclosable Matter (as defined below) according to this policy and to adopt the attitude 'when in doubt, report'. We are committed to identifying and responding to each Disclosable Matter, and supporting anyone who decides to report it.
- 1.1.3. We take all reports seriously, so it is important that you do not make reports which you know to be untrue.
- 1.1.4. This policy outlines the procedure for our management of a Disclosable Matter.

**1.2. Related policies**

- 1.2.1. This policy should be read in conjunction with the following Device Technologies Group policies:
  - Code of Conduct (DTP-0001)
  - Anti-Bribery and Corruption Policy (DTP-0119)
  - Gifts and Entertainment Policy (DTP-0120)
  - Bullying Discrimination and Harassment Policy (DTP-1623)
  - Supplier Code of Conduct (DTP-2807)
  - Modern Slavery and Human Rights Policy (DTP-2806)
  - Doing the Right Thing Policy (DTP-1607)

**WHISTLEBLOWER POLICY****1.3. Availability**

1.3.1. A copy of this policy is available:

- On the QA Document Library of hub portal.
- On the Public Policy Library page of DT.
- Through the Employee Code of Conduct; and via training for new starters

**1.4. DEFINITIONS**

- AFP: Australia Federal Police as defined in the Australian Federal Police Act 1979 (Cth).
- APRA: Australian Prudential Regulation Authority.
- ASIC: Australian Securities and Investments Commission.
- Corporations Act: the Corporations Act 2001 (Cth).
- Taxation Administration Act: The Taxation Administration Act 1953 (Cth).

**2. APPLICATION OF THIS POLICY**

2.1. This policy applies to you if you are any of the following:

- 2.1.1. A current, or former, employee or officer of Device Technologies Group (including permanent, part-time, fixed term or temporary, interns, secondees, managers, and directors);
- 2.1.2. A supplier of services or goods to Device Technologies Group (whether paid or unpaid), including their employees (for example, current and former contractors, consultants, service providers and business partners);
- 2.1.3. An associate of Device Technologies Group; or
- 2.1.4. A relative, dependant or spouse of an individual described in the above paragraphs (for example, relatives, dependants or spouse of current and former employees, contractors, consultants, service providers, suppliers and business partners).

2.2. This policy applies whether you are at work or engaged in any work-related activity. It is not restricted in its operation to work hours or your usual place of work. It applies at conferences, work functions, work related social events, and business trips.

**3. DISCLOSABLE MATTER**

3.1. A Disclosable Matter is information which you have reasonable grounds to suspect concerns misconduct, or an improper state of affairs or circumstances, in relation to Device Technologies Group, a related body corporate of Device

**WHISTLEBLOWER POLICY**

Technologies Group, or our business (including in relation to an officer or employee of Device Technologies Group or of any related body corporate of it).

- 3.2. A Disclosable Matter includes conduct which you have reasonable grounds to suspect was engaged in by an entity or person named in paragraph 3.1, and which:

3.2.1. Breaches the Corporations Act, the Australian Securities and Investments Commission Act 2001 (Cth), the Banking Act 1959 (Cth), the Financial Sector (Data Collection) Act 2001 (Cth), the Insurance Act 1973 (Cth), the Life Insurance Act 1995 (Cth), the National Consumer Credit Protection Act 2009 (Cth), or the Superannuation Industry (Supervision) Act 1993 (Cth);

3.2.2. Is an offence against any other law of the Commonwealth of Australia that is punishable by imprisonment for a period of 12 months or more; or

3.2.3. Indicates a significant risk to public safety or the stability of, or confidence in, the financial system (even if it does not involve a breach of a particular law).

- 3.3. A Disclosable Matter includes conduct that may not involve contravention of a particular law.

- 3.4. By way of example only, a Disclosable matter may include misconduct or serious wrongdoing that you reasonably believe:

3.4.1. Is dishonest, illegal, fraudulent, corrupt or unsafe;

3.4.2. Is unethical, including any conduct that would breach our Code of Conduct;

3.4.3. Involves irregular use of company funds or practices (including misleading accounting or financial reporting practices);

3.4.4. Is impeding internal controls, or internal or external audit processes;

3.4.5. Involves misuse of our business information;

3.4.6. Is damaging to our business, financial position or reputation;

3.4.7. Poses a significant risk to the stability of the financial system;

3.4.8. Endangers the health and safety of any employee or member of the public; or

3.4.9. Poses a significant risk to the environment.

**4. THIS POLICY DOES NOT APPLY TO CERTAIN MATTERS**

- 4.1. This policy and the whistleblower protections in the Corporations Act do not apply to a disclosure which is solely about a personal work-related grievance, where the grievance:

4.1.1. Concerns your current or former employment, and has (or tends to have) implications for you personally;

## WHISTLEBLOWER POLICY

- 4.1.2. Has no significant implications for Device Technologies Group or its related body corporate that do not relate to you; and
- 4.1.3. Does not concern actual or alleged conduct described in paragraph 3.2, and does not breach laws against whistleblower-related victimisation.
- 4.2. Subject to paragraph 4.3, a personal work-related grievance may include the following:
  - 4.2.1. An interpersonal conflict between you and another employee;
  - 4.2.2. A decision relating to your terms and conditions of engagement, or to your engagement, transfer or promotion; and
  - 4.2.3. A decision to suspend or terminate your engagement, or otherwise pursue a disciplinary sanction.
- 4.3. A personal work-related grievance may still qualify for protection under this policy and the whistleblower protections in the Corporations Act if:
  - 4.3.1. It includes information about actual or alleged conduct described in clause 3.2.
  - 4.3.2. it relates to information which suggests misconduct beyond your personal circumstances; or
  - 4.3.3. It relates to a breach of laws against whistleblower-related victimisation.
- 4.4. If you wish to report a personal work-related grievance, please refer to the Doing the Right Thing Policy.
- 4.5. Disclosures that are not about a Disclosable Matter do not qualify for protection under this policy, the Corporations Act or the Taxation Administration Act.

## 5. HOW TO MAKE A REPORT

- 5.1. You should report a Disclosable Matter as soon as you become aware of it. If you wish to seek additional information before formally reporting a Disclosable Matter, you may contact Device Technologies Group's Whistleblower Protection Officer, being the Compliance and Risk Manager or email [whistleblower@device.com.au](mailto:whistleblower@device.com.au), or an independent lawyer.
- 5.2. In the first instance, you should report a Disclosable Matter to Device Technologies Group's Eligible Recipients, being the nominated officers or senior managers:

Position	Name	Phone	Email
<b>Compliance and Risk Manager</b>	Stewart Nicotra	61490386656	<a href="mailto:snicotra@device.com.au">snicotra@device.com.au</a> or <a href="mailto:whistleblower@device.com.au">whistleblower@device.com.au</a>
<b>Chief Financial Officer</b>	Ben Arthur	61404067685	<a href="mailto:ben.arthur@device.com.au">ben.arthur@device.com.au</a>

## WHISTLEBLOWER POLICY

**General Manager –  
Commercial Operations**

Paul Kellick

61413010314

[pkellick@device.com.au](mailto:pkellick@device.com.au)

You may also post a report to the following address, marked to the attention of one of the Eligible Recipients above:

CONFIDENTIAL: *[Name & Position of Eligible Recipient]*

Device Technologies Group

1 Garigal Road,

Belrose, NSW, 2085

Australia

5.2.1. An auditor or actuary of Device Technologies Group; or

5.2.2. The dedicated external service provider through

[www.device.ethicspoint.com](http://www.device.ethicspoint.com)

5.3. To qualify for whistleblower protection under the Corporations Act (or, where relevant, the Taxation Administration Act), your report under paragraph 5.2 must be made directly to a person specified in paragraph 5.2.

5.4. You may also report a Disclosable Matter to ASIC, APRA, another Commonwealth body prescribed by regulation or the Commissioner of Taxation (if you consider the information may assist the Commissioner to perform his or her functions or duties in relation the tax affairs of Device Technologies Group or an associate of Device Technologies Group). This report will qualify for whistleblower protection under the Corporations Act or, where applicable, the Taxation Administration Act.

5.5. You may report a Disclosable Matter to a lawyer for the purpose of obtaining legal advice or representation relating to the operation of the whistleblower provisions in the Corporations Act or the Taxation Administration Act. This report is protected even if the lawyer concludes that it does not relate to a Disclosable Matter.

5.6. Your report can be made anonymously (see paragraph 09).

## 6. PUBLIC INTEREST OR EMERGENCY DISCLOSURE

6.1. You must not report a Disclosable Matter to a member of parliament or a journalist, unless it is a public interest disclosure or an emergency disclosure.

6.2. To make a public interest disclosure:

6.2.1. You must have previously reported the Disclosable Matter to a regulator specified in paragraph 5.45.4, and at least 90 days must have passed since that previous report;

6.2.2. After that 90-day period, you must give the regulator who received that previous report, a written notice that:

- Includes sufficient information to identify your previous report; and

**WHISTLEBLOWER POLICY**

- States that you intend to make a public interest disclosure;
  - 6.2.3. You must not have reasonable grounds to believe that action is being, or has been, taken to address the matters relating to the previous report;
  - 6.2.4. You must have reasonable grounds to believe that making a further report to a member of parliament or journalist would be in the public interest; and
  - 6.2.5. You must disclose information to the member of parliament or a journalist only to the extent necessary to inform him or her of the Disclosable Matter.
- 6.3. To make an emergency disclosure:
- 6.3.1. You must have reasonable grounds to believe that the Disclosable Matter concerns a substantial and imminent danger to the health or safety of one or more persons or to the natural environment;
  - 6.3.2. You must have previously reported the Disclosable Matter to a regulator specified in paragraph 5.4, and you must also subsequently give it a written notice that:
    - Includes sufficient information to identify your previous report; and
    - States that you intend to make an emergency disclosure; and
  - 6.3.3. You must disclose information to the member of parliament or a journalist only to the extent necessary to inform him or her of the substantial and imminent danger.
- 6.4. It is important for you to understand the above criteria for making a public interest disclosure or an emergency disclosure.

**7. HANDLING AND INVESTIGATING A REPORT OF DISCLOSABLE MATTER**

- 7.1. You should contact an independent lawyer before making a public interest disclosure or an emergency disclosure.
- 7.2. If you report a Disclosable Matter under paragraph 5.2 to a person who works at Device Technologies Group, where possible, you will be notified within 05 days that your report has been received.
- 7.3. You should not attempt to investigate any Disclosable Matter yourself.
- 7.4. Device Technologies Group will need to assess your report to determine:
  - 7.4.1. Whether it qualifies for protection; and
  - 7.4.2. Whether a formal, in-depth investigation is required.
- 7.5. We will respond to any report of a Disclosable Matter where we believe that it was made on reasonable grounds.



**WHISTLEBLOWER POLICY**

- 7.6. Whilst our process and timing may vary depending on the nature of the Disclosable Matter, these are the key steps generally involved if we investigate a report of a Disclosable Matter:
- 7.6.1. Within 30 days after receiving your report, we may:
- Conduct an internal investigation into the substance of your report; or
  - Appoint an external investigator to determine whether there is evidence to support the matters raised in your report.
- 7.6.2. We may also take such other steps as we consider reasonably appropriate to properly assess your report and to determine appropriate outcomes.
- 7.6.3. You may be asked to provide additional information to assist any assessment or investigation of your report, including a description of the facts and circumstances of the misconduct or improper state of affairs or circumstances.
- 7.6.4. We will decide what steps should be taken to address any verified misconduct or improper state of affairs or circumstances.
- 7.6.5. You will receive feedback on the progress or outcome of the assessment or investigation (subject to privacy and confidentiality restrictions).
- 7.7. Without your consent, we cannot disclose information that is likely to lead to your identification as part of our investigation process, unless:
- 7.7.1. The information does not include your identity;
- 7.7.2. We remove all information relating to your identity or other information that is likely to lead to your identification (for example, your name, position title and other identifying details); and
- 7.7.3. It is reasonably necessary for investigating the issues raised in your report.
- 7.8. We acknowledge the limitations of our investigation process. We may not be able to undertake an investigation if we are not able to contact you (for example, if the report is made anonymously and you have refused to provide, or have not provided, a means of contacting you).
- 7.9. We will provide you with regular updates if you can be contacted (including through anonymous channels). The frequency and timeframe may vary depending on the nature of your report.
- 7.10. The method for documenting and reporting the findings from an investigation will depend on the nature of the report. Those findings will be documented and reported to those responsible for oversight of this policy. In doing so, we will preserve confidentiality by taking measures described in paragraph 09.

**WHISTLEBLOWER POLICY**

- 7.11. At the end of the investigation, you will be informed of the outcome of the investigation, unless circumstances are such that it may not be appropriate to provide details of the outcome to you.

**8. WHAT PROTECTIONS WILL A WHISTLEBLOWER RECEIVE?**

- 8.1. We are committed to protecting and supporting whistleblowers who report a Disclosable Matter according to this policy. If you report this, the following protections are in place to protect you:
- 8.1.1. Identity protection (confidentiality) (see paragraph 09);
  - 8.1.2. Protection from detrimental acts or omissions (see paragraph 10);
  - 8.1.3. Compensation and other remedies (see paragraph 11); and
  - 8.1.4. Civil, criminal and administrative liability protection (see paragraph 12).
- 8.2. Those protections apply not only to internal disclosures, but to disclosure to lawyers, regulatory and other external bodies, and public interest disclosures and emergency disclosures described in paragraph 6.
- 8.3. You can still qualify for protection even if your disclosure turns out to be incorrect.

**9. IDENTITY PROTECTION (CONFIDENTIALITY)**

- 9.1. Your report can be made anonymously and still be protected under the Corporations Act, or where applicable, the Taxation Administration Act.
- 9.2. You can choose to remain anonymous while making a report, over the course of the investigation and after the investigation is finalised. You can refuse to answer questions that you feel could reveal your identity at any time, including during follow-up conversations. If you wish to remain anonymous, you should maintain ongoing two-way communication with Device Technologies Group, so that Device Technologies Group can ask follow-up questions or provide feedback.
- 9.3. If you choose to remain anonymous, the most practical way to protect your anonymity is to contact us via an anonymised email address or lodge a report through the dedicated external service provider available at [www.device.ethicspoint.com](http://www.device.ethicspoint.com). If we need to speak to you to investigate your report, we will advise you how we propose to do that and maintain your anonymity.
- 9.4. You may adopt a pseudonym for the purpose of your report. This may be appropriate where your identity is known to your supervisor or the Whistleblower Protection Officer, but you prefer not to disclose your identity to others.



**WHISTLEBLOWER POLICY**

- 9.5. All information disclosed in your report, including your identity (where you choose not to disclose this), will remain confidential to the extent required by law.
- 9.6. If you report a Disclosable Matter under this policy, a person cannot disclose your identity or information that is likely to lead to your identification (which the person obtained directly or indirectly because of your report), except under paragraph 9.6.1 or 9.6.2 below.
- 9.6.1. A person can disclose your identity:
- To ASIC, APRA or a member of the AFP or (for tax-related disclosures) to the Commissioner of Taxation; and
  - To a lawyer (for the purposes of obtaining legal advice or legal representation about the whistleblower provisions in the Corporations Act or Taxation Administration Act);
  - A person or body prescribed by regulations; or
  - With your consent.
- 9.6.2. A person can disclose information contained in your report, with or without your consent, if:
- The information does not include your identity;
  - We have taken all reasonable steps to reduce the risk that you will be identified from the information; and
  - It is reasonably necessary for investigating the issues raised in your report.
- 9.7. It is illegal for a person to disclose your identity or information that is likely to lead to your identification, except under paragraph 9.6.1 or 9.6.2 above. You may lodge a complaint about a breach of confidentiality with:
- 9.7.1. The Compliance and Risk Manager directly or [whistleblower@device.com.au](mailto:whistleblower@device.com.au); or
- 9.7.2. A regulator, such as ASIC, APRA or the Australian Taxation Office, for investigation.
- 9.8. Measures that we will take to protect your identity include the following:
- 9.8.1. All personal information or references to you will be redacted in relevant documents;
- 9.8.2. Where possible, we will consult with you to identify any aspects of your report that could inadvertently identify you;
- 9.8.3. Disclosures will only be handled and investigated by qualified staff;
- 9.8.4. All paper and electronic documents and other materials relating to the disclosure will be stored securely;

**WHISTLEBLOWER POLICY**

9.8.5. Access to information relating to the disclosure will be limited to those directly involved in managing and investigating the disclosure; and

9.8.6. 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.

**10. PROTECTION FROM DETRIMENTAL ACTS OR OMISSIONS**

10.1. If you report a Disclosable Matter under this policy, there are legal protections for protecting you (or any other person) from detriment in relation to your report.

10.2. Your position and duty within our business will not be altered to your detriment or disadvantage as a result of making your report. You will not be otherwise dismissed, demoted, harassed, discriminated against, or subject to bias as a result of making your report.

10.3. A person cannot engage in conduct that causes detriment to you (or another person), in relation to your report, if:

10.3.1. The person believes or suspects that you (or another person) made, may have made, proposes to make or could make a report that qualifies for whistleblower protection; and

10.3.2. The belief or suspicion is the reason, or part of the reason, for the conduct.

10.4. A person cannot make a threat to cause detriment to you (or another person) in relation to your report. A threat may be express or implied, or condition or unconditional. If you or another person have or has been threatened, it is not a requirement for you or the other person to actually fear that the threat will be carried out.

10.5. Detrimental conduct that is prohibited under the law includes:

10.5.1. Dismissal of an employee;

10.5.2. Injury of an employee in his or her employment;

10.5.3. Alteration of an employee's position or duties to his or her disadvantage;

10.5.4. Discrimination between an employee and other employees of the same employer;

10.5.5. Harassment or intimidation of a person;

10.5.6. Harm or injury to a person, including psychological harm;

10.5.7. Damage to a person's property;

10.5.8. Damage to a person's reputation;

10.5.9. Damage to a person's business or financial position; or

**WHISTLEBLOWER POLICY**

10.5.10. Any other damage to a person.

10.6. Examples of actions that are not detrimental conduct include:

10.6.1. Administrative action that is reasonable for the purpose of protecting a discloser from detriment (for example, moving a discloser who has made a disclosure about their immediate work area to another location to prevent them from detriment); and

10.6.2. Managing a discloser's unsatisfactory work performance, if the action is in line with Device Technologies Group's performance management framework.

10.7. To the extent it is reasonable and practical to do so, we will monitor and manage the behaviour of any people who are involved in your report.

10.8. We will take all reasonable precautions to ensure that you (and your colleagues and relatives) are not harmed, injured, intimidated, harassed, bullied or victimised by any of our employees, officers, contractors, suppliers, consultants and directors.

10.9. We will consider any reasonable requests for additional protections that you may make or we consider necessary for your protection (for example, leave of absence during any investigation).

10.10. If you believe you have suffered detriment, you may seek independent legal advice or contact regulatory bodies such as ASIC, APRA or the Australian Taxation Office.

10.11. An employee who causes, or threatens to cause, detriment to any suspected whistleblower (being a person whom the employee suspects has reported or will report a Disclosable Matter) may be subject to disciplinary action under our Doing the Right Thing Policy. The employee may also be subject to court orders under the Corporations Act or, where applicable, the Taxation Administration Act, including an order to:

10.11.1. Require the employee to compensate the suspected whistleblower, or any other person, for loss, damage or injury as a result of the detrimental conduct, or (jointly with Device Technologies Group) for loss, damage or injury as a result of the detrimental conduct;

10.11.2. Grant an injunction to prevent, stop or remedy the effects of the detrimental conduct;

10.11.3. Require the employee to apologise to the suspected whistleblower for engaging in the detrimental conduct;

**WHISTLEBLOWER POLICY**

10.11.4. Reinstate to the same position or a position at a comparable level, the suspected whistleblower who was terminated from a particular position; or

10.11.5. Require the employee to pay exemplary damages to the suspected whistleblower or to any other person.

**11. COMPENSATION AND OTHER REMEDIES**

11.1. You (or any other employee or person) can seek compensation and other remedies through the courts:

11.1.1. For suffering loss, damage or injury because you reported a Disclosable Matter under this policy; and

11.1.2. If Device Technologies Group failed to take reasonable precautions and exercise due diligence to prevent the detrimental conduct.

11.2. You should seek independent legal advice on compensation or other remedies that may be available.

**12. CIVIL, CRIMINAL AND ADMINISTRATIVE LIABILITY PROTECTION**

12.1. You are protected from any of the following in relation to your report of a Disclosable Matter under this policy:

12.1.1. Civil liability (for example, any legal action against you for breach of an employment contract, duty of confidentiality or another contractual obligation);

12.1.2. Criminal liability (for example, attempted prosecution of you for unlawfully releasing information, or other use of your report against you in a prosecution (other than for making a false disclosure)); and

12.1.3. Administrative liability (for example, disciplinary action for making the report).

12.2. The above protections do not grant immunity for any misconduct you have engaged in that is revealed in your report. For more information, you should seek independent legal advice before making your report.

**WHISTLEBLOWER POLICY****13. ENSURING FAIR TREATMENT OF INDIVIDUALS MENTIONED IN A DISCLOSURE**

13.1. Measures that we will take to ensure fair treatment of our employees who are mentioned in any report of a Disclosable Matter under this policy, or who are the subject of any such report, include the following:

13.1.1. Disclosures will be handled confidentially, when it is practical and appropriate in the circumstances.

13.1.2. Each disclosure will be assessed and may be the subject of an investigation;

13.1.3. An employee who is the subject of a disclosure will be advised about the subject matter of the disclosure where required by principles of natural justice and procedural fairness, and before any actions are taken; and

13.1.4. An employee who is the subject of a disclosure may use Device Technologies' Employee Assistance Plan (Access EAP), details available at <http://www.accesseap.com.au/client-area/client-login.html> .

**14. EVALUATION AND REVIEW**

14.1. The Compliance and Risk Manager is responsible for monitoring, reporting and reviewing this policy, and will ensure that:

14.1.1. This policy is reviewed at least once every 02 years by the Ethics and Compliance Committee; and

14.1.2. Compliance with this policy is monitored regularly, and the effectiveness of this policy is reported to Ethics and Compliance Committee.

14.2. This policy may be amended by resolution of the Ethics and Compliance Committee.

**WHISTLEBLOWER POLICY**
**Appendix A**

Country	Whistleblowing Protections	Relevant Law
<b>Hong Kong</b>	No specific overarching protections apply to whistleblowers generally (although there are various piecemeal legislative provisions that apply in certain contexts (e.g. money laundering and the prevention of bribery)). Save where one of these specific provisions is triggered, any impact to employees who are involved in or impacted by a report made under a whistleblowing policy should be considered under the Employment Ordinance, taking into account the common law principles of fairness and natural justice.	N/A
<b>Singapore</b>	There is no overarching whistleblowing law. There are anti-corruption provisions that safeguard the identity of those individuals that provide information that lead to an investigation and prosecution of any offences under the Act.	Prevention of Corruption Act 1960 section 36
<b>New Zealand</b>	The law attempts to protect an employee who makes a disclosure not only from any criminal or civil lawsuit, but also from retaliation from their employer. Employee extends to contractor, volunteers etc. Anonymity is only legally protected in some cases.	Protected Disclosures Act 2000
<b>Vietnam</b>	Whistleblowers and their relatives are protected by certain legal mechanisms. Although they give their name and address when making complaint, their identifying information must be kept confidential. Written	Denunciation No. 03/2011/QH13 and the Anti-Corruption Law.



## WHISTLEBLOWER POLICY

	conclusion must occur within a period up to 60 days. This may be extended for an additional period up to 150 days total, subject to the complexity of the case. The conclusion must be disclosed publicly in accordance with the laws.	
<b>Thailand</b>	There is no dedicated whistleblower legislation for employees. To have anonymity protected, a whistleblower needs to be deemed a witness entitled to protection under the laws on witness protection and anti-corruption.	Executive Measures in Anti-Corruption Act, B.E. 2551, and Witness Protection Act
<b>Malaysia</b>	Whistleblowers can disclose an act of improper conduct, to the relevant enforcement agency (i.e. Malaysia Anti-Corruption Commission), that may enable the enforcement agency to initiate an investigation. The whistleblower's identity must not be disclosed, and protections will be provided. Protection is also given to those who have connection / relationship with the whistleblower. These protections are treated as formal disclosures and are not specific to employees. Generally, anonymous disclosures are not accepted.	Whistleblower Protection Act 2010
<b>Philippines</b>	There is no dedicated whistleblower law.	N/A
<b>Indonesia</b>	There are protections for employees who have knowledge of criminal acts of the employer, however no general protections apply for whistleblowers. A company policy on whistleblowing must be socialised with employees before being filed with and ratified by the Ministry of Manpower and Transmigration.	Implementing Community Participation and Providing Rewards in the Prevention and Eradication of Acts of Corruption ("GR No. 43/2018")