



**Defence**  
Bank

# Policy - Whistleblower Protection.

**Owner:** Chief People Officer  
**Effective date:** 30 June 2024  
**Version:** 1.4.

[defencebank.com.au](https://defencebank.com.au) | 1800 033 139 | Defence Bank App | In Branch

Defence Bank Limited ABN 57 087 651 385 | AFSL/Australian Credit Licence 234582

## Contents.

|   |           |
|---|-----------|
| <b>Why this is important.</b>   | <b>1</b>  |
| <b>What is the purpose of this policy.</b>                            | <b>1</b>  |
| <b>Who this applies to and when.</b>                                  | <b>1</b>  |
| <b>Definitions.</b>   | <b>1</b>  |
| <b>Requirements.</b>  | <b>2</b>  |
| What reports are protected under this policy?                         | 2         |
| Who is an Eligible Whistleblower?                                     | 2         |
| What must a Whistleblower report be about?                            | 3         |
| What is Wrongdoing?   | 3         |
| Examples of conduct that may be reported as Wrongdoing.               | 3         |
| What should I do if I have a personal work-related grievance?         | 4         |
| Making a Protected Report.  | 4         |
| How can a Whistleblower report be made?                               | 4         |
| Can I remain anonymous when making a report?                          | 5         |
| Disclosure to be made with reasonable grounds.                        | 6         |
| False reporting.  | 6         |
| Protection and support available to Whistleblowers.                   | 6         |
| Protecting the Whistleblower's identity.                              | 6         |
| Protection against detrimental conduct.                               | 7         |
| Protection for Whistleblowers against litigation.                     | 8         |
| Other support available for Whistleblowers.                           | 8         |
| How we handle Protected Reports.                                      | 9         |
| How do we investigate reports of Wrongdoing?                          | 9         |
| Treatment of employees who are the subject of a Whistleblower report. | 10        |
| Internal reviews.   | 10        |
| Reporting to the Board.   | 11        |
| Review, Access and Training in relation to this policy.               | 11        |
| <b>Roles and responsibilities.</b>                                    | <b>11</b> |
| <b>Breaches.</b>  | <b>12</b> |
| <b>Contacts for questions and more information.</b>                   | <b>12</b> |



**Document information. .... 13**

**Document history. .... 13**

**Appendix 1. .... 14**

    Who can a Protected Report be made to? ..... 14

    Public interest disclosures. .... 14

    Emergency disclosures..... 15

    Personal work-related grievances. .... 15



## Why this is important.

1. Defence Bank is committed to a culture of legal and ethical behaviour and good corporate governance, and creating a workplace environment where employees feel safe to raise concerns of Wrongdoing that they have witnessed or reasonably believe has or is occurring.
2. Defence Bank encourages all employees who have concerns about possible Wrongdoing or inappropriate behaviour at Defence Bank to raise those concerns in the ordinary course of business. You can do this by contacting your People Leader or People & Capability.
3. There may be times when you do not feel comfortable speaking up in the ordinary course of business, would like to raise your concerns anonymously, or feel that you need confidentiality and protection. In these circumstances, Defence Bank encourages you to raise concerns about Wrongdoing in accordance with this Whistleblower Protection Policy.
4. This policy is an important tool for helping Defence Bank to identify any Wrongdoing that may not be uncovered unless there is a safe and secure means for disclosing it.
5. This policy is underpinned by our corporate principles of being Accountable, Collaborative and Transparent which guide our behaviour and apply to every aspect of Defence Bank's business.

## What is the purpose of this policy.

6. The purpose of this policy is to:
  - a. encourage genuine concerns about possible Wrongdoing in relation to Defence Bank to be raised as soon as possible;
  - b. provide guidance in relation to how to raise those concerns, and how they will be investigated and the support available to individuals raising concerns under this policy;
  - c. ensure that individuals who disclose Wrongdoing can do so safely, securely and with confidence that they will be protected and supported; and
  - d. comply with requirements under the Corporations Act and the Taxation Administration Act and APRA Prudential Standard 520 (Fit and Proper) to enable disclosures of Wrongdoing and ensure statutory protection is afforded to anyone who makes a Protected Report.

## Who this applies to and when.

7. This Policy applies to everyone at Defence Bank, including all directors, employees, contractors and consultants. It also applies to any person who is in one of the categories of people set out in clause 10.

## Definitions.

8. In this Policy:

**APRA** means Australian Prudential Regulation Authority.

**ASIC** means Australian Securities & Investments Commission.

**ASIC Act** means *Australian Securities and Investments Commission Act 2001* (Cth).

**ATO** means the Australian Taxation Office.

**Corporations Act** means *Corporations Act 2001* (Cth).

**Detriment** has the meaning specified in clause 31.

**Nominated Officer** means a person appointed by Defence Bank as the preferred recipient of internal disclosures made under this policy. The Nominated Officers' details are set out in clause 15.

**Protected Report** is defined in clause 9.

**Taxation Administration Act** means *Taxation Administration Act 1953* (Cth).

**Whistleblower** means a person who falls within one of the categories described in clause 10 of this policy and who makes a report of Wrongdoing, based on reasonable grounds, to one of the people described in clause 15.

**Wrongdoing** is defined in clause 11 and 12.

## Requirements.

### What reports are protected under this policy?

9. To be eligible for the legal protections outlined in this policy, you must:
  - a. be an eligible whistleblower (see clause 10);
  - b. report your concerns to an eligible recipient, to Your Call, or to certain other persons (see clause 15); and
  - c. have reasonable grounds to suspect Wrongdoing in relation to Defence Bank (see clause 15).

If your report meets all three of the above these criteria, it is a **Protected Report**.

If your report doesn't meet the above criteria, we still encourage you to raise your concerns with us. However, only Protected Reports receive the legal protections outlined in this policy.

### Who is an Eligible Whistleblower?

10. You are an eligible whistleblower if you are currently, or previously have been, either:
  - a. an officer of Defence Bank;
  - b. an employee of Defence Bank, including any interns or secondees;
  - c. a person who supplies goods or services to Defence Bank, whether paid or unpaid, or an employee of such a person;
  - d. an associate of Defence Bank, or
  - e. a spouse, relative or dependent of a person referred to above.

## What must a Whistleblower report be about?

### What is Wrongdoing?

11. For the report to be a Protected Report, one of the requirements is that the eligible whistleblower making the report has reasonable grounds to suspect Wrongdoing is occurring or has occurred. It is not possible to provide an exhaustive list of the activities which should be reported for the purpose of this policy. Generally, Wrongdoing includes any conduct which an eligible whistleblower has reasonable grounds to suspect:
  - a. is about misconduct or an improper state of affairs or circumstances concerning Defence Bank;
  - b. is about misconduct or an improper state of affairs or circumstances in relation to the tax affairs of Defence Bank or an associated company which the eligible whistleblower considers may assist to perform the functions or duties in relation to the tax affairs of Defence Bank;
  - c. indicates that Defence Bank or any of its officers or employees has engaged in conduct that:
    - i. involves a breach of or is an offence against any of the following Commonwealth laws: the *Corporations Act 2001*, the *ASIC Act 2001*, the *Banking Act 1959*, the *Financial Sector (Collection of Data) Act 2001*, or the *National Consumer Credit Protection Act 2009*, or regulations made under those laws;
    - ii. is an offence against any other Commonwealth law that is punishable by imprisonment of 12 months or more;
    - iii. indicates a systemic issue that a relevant regulator (e.g. ASIC or APRA) should know about to properly perform its functions;
    - iv. indicates a significant risk to public safety or the stability of, or confidence in, the financial system, even if it does not involve breach of a particular law; or
    - v. is indicative of dishonest or unethical behaviour or practices that may cause consumer harm.

These matters are referred to as ‘**Wrongdoing**’ in this policy.

### Examples of conduct that may be reported as Wrongdoing.

12. Examples of the types of matters that may be reportable as Wrongdoing include, but are not limited to:
  - a. Fraud (including dishonest activity, deliberate falsification, knowingly publishing or providing documentation that is false, misappropriation of funds, covering up fraud);
  - b. Corrupt behaviour (including bribery, dishonestly failing to act or dishonestly taking advantage of an employment position);
  - c. Conduct leading to unfair customer outcomes;
  - d. Misconduct or unethical behaviour (including discrimination, sexual harassment and serious breaches of Defence Bank’s Code of Conduct and workplace policies);

- e. Legal or regulatory non-compliance (including breaches of financial services laws, Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF) laws, Modern Slavery laws);
- f. Illegal conduct, such as theft, dealing in, or use of illicit drugs, violence or threatened violence, and criminal damage against property;
- g. Unsafe work practices or not properly responding to a serious safety issue;
- h. Serious inappropriate or unethical conduct such as gross mismanagement, serious and substantial waste of company resources or repeated breaches of administrative procedures;
- i. Taking or threatening to take detrimental action against a person who has made a disclosure or is suspected to have made, or planning to make a disclosure;
- j. Deliberate concealment of information tending to show any of the matters listed above.

Generally, Wrongdoing does not include personal work-related grievances. See clause 13.

## What should I do if I have a personal work-related grievance?

- 13. We encourage everyone to speak up about concerns. However, reports that relate solely to personal work-related grievances are not generally considered to be Wrongdoing and are therefore not covered by this policy.
  - a. Personal work-related grievances typically relate to an individual's current or former employment arrangements, performance, remuneration outcomes or personal circumstances that do not have significant implications for the organisation (for example an interpersonal conflict between you and another employee, or a decision about your employment that does not breach workplace laws).
  - b. Personal work-related grievances should be internally raised using the Grievance policy. Sometimes, a disclosure of a personal work-related grievance can also be a Protected Report. See Appendix 1 for more information.

## Making a Protected Report.

### How can a Whistleblower report be made?

- 14. We encourage you to report actual or suspected Wrongdoing to us as soon as you become aware of it. Defence Bank would like to identify and address any Wrongdoing as soon as possible.
- 15. You are encouraged to make a report to one of our Nominated Officers. Our Nominated Officers are:

| Name           | Role                    |
|----------------|-------------------------|
| Kristen Bugeja | Chief People Officer    |
| Mano Simos     | Chief Risk Officer      |
| Dean Barton    | Chief Financial Officer |

- a. By email on our confidential channel: [speakup@defencebank.com.au](mailto:speakup@defencebank.com.au)



16. Alternatively, you may make a report using our whistleblowing service, Your Call. Your Call is an external, independent provider that provides confidential reporting of Whistleblower concerns relating to this policy. Reporting to Your Call also enables your report to be made anonymously if you choose to do so. You can make a Whistleblower report to Your Call:
- b. Online: <https://www.yourcall.com.au/report> You will be required to enter Defence Bank's unique identifier code **DEF833205**.
  - c. By phone using Your Call's external reporting hotline: 1300 790 228 (9am to midnight AEST on business days).

#### **How Your Call works.**

Your Call uses an online message board which you will have access to after making the report. The message board allows you to:

- i. communicate with Your Call and with Defence Bank with or without revealing your identity;
- ii. securely upload any relevant documentation and/or material that you wish to provide;
- iii. receive updates; and
- iv. request support or report detriment.

Your Call will provide the Nominated Officers with a copy of your report and any relevant documents or records provided by you to Your Call. If your report relates to a Nominated Officer, Your Call will exclude that person from all communications when Your Call provide information about your report to us.

How to use Your Call if you have a speech or hearing impairment.

- i. If you are deaf or have a hearing or speech impairment, you can contact Your Call online. If you would like to contact Your Call by phone, you can do so through the National Relay Service. Simply choose your contact method at [www.relayservice.gov.au](http://www.relayservice.gov.au) and request Your Call's hotline 1300 790 228.
17. You can also make a report in person, in writing, verbally or by telephone directly to any of the people listed in Appendix 1.

#### **Can I remain anonymous when making a report?**

18. You can remain anonymous when making a Protected Report. There is no requirement to provide your name or identify yourself at any stage during the reporting or investigation process or after the investigation is finalised. You can also decide not to answer questions that you feel may reveal your identity. You can also choose to provide your identity to the person that you are making the report to but not consent to them sharing your identity with anyone else.
19. We will respect your right not to identify yourself. However, if you choose to remain anonymous, this may affect the ability of Defence Bank to investigate and properly communicate with you about the report.



20. Defence Bank encourages disclosers who would prefer to remain anonymous to maintain ongoing two-way communication with Defence Bank so that Defence Bank can ask follow up questions and provide feedback. This can also be done using the Your Call service which provides for ongoing anonymous communication.

#### **Disclosure to be made with reasonable grounds.**

21. To be a Protected Report, your disclosure must be made with reasonable grounds. In practice, this means that there is more than just a suspicion of potential Wrongdoing and there is some information that supports the allegation. You do not need to prove the allegations, but you are encouraged to provide evidence in support of your disclosure if it is safely available.
22. An eligible whistleblower can still qualify for protection even if their Protected Report turns out to be incorrect or unsubstantiated, provided they have a reasonable basis for making the report.

#### **False reporting.**

23. False reporting will be treated seriously. If we find that you have intentionally made a false report (for example, if you know a report is untrue and you report it to harm, annoy, or cause distress to someone), we may take disciplinary action against you, which may include termination of your employment or engagement with us.

#### **Protection and support available to Whistleblowers.**

24. If you make a Protected Report, you are entitled to the benefit of certain protections in accordance with the *Corporations Act* or the *Taxation Administration Act*. These protections apply regardless of whether you make a Protected Report to one of our Nominated Officers, to Your Call or to another entity specified in Appendix 1, such as ASIC or APRA.

#### **Protecting the Whistleblower's identity.**

25. If you make a Protected Report, your disclosure will be treated as confidential in accordance with legal requirements.
26. If you make a Protected Report, it is illegal for a person to disclose your identity or information that is likely to lead to identification of your identity, unless:
- a. you give your consent;
  - b. the disclosure is required by law; or
  - c. the disclosure is made to:
    - i. a professional legal advisor (including Defence Bank's legal team) for the purpose of obtaining legal advice or representation; or
    - ii. authorised regulatory bodies, such as ASIC, APRA or a member of the Australian Federal Police.
    - iii. A person who is dealing with a Protected Report may disclose information that is reasonably necessary for the purposes of investigating the report, provided that the information does not include your identity. If this happens, reasonable steps will be taken to reduce the risk that you will be identified as a result of the report (for example by removing your personal information or other details that are likely to identify you).

27. To maintain confidentiality of a Whistleblower's identity, Defence Bank will:
- ensure personal information or references to the Whistleblower's identity is redacted in all investigation and reporting documents;
  - refer to the Whistleblower in gender-neutral terms;
  - where possible, contact the Whistleblower to help identify certain aspects of their disclosure that could inadvertently identify them;
  - ensure that the information a Whistleblower provides and all materials relevant to a Protected Report are held securely with access limited only to the individuals necessary to investigate your Protected Report, and to support and protect the Whistleblower; and
  - take reasonable steps to ensure its personnel understand the requirements of this policy.
28. You should also be aware that during an investigation, it may be necessary for us to tell the people who are believed to be involved in the Wrongdoing about the alleged Wrongdoing. This is to ensure a fair investigation and provide those people with an opportunity to respond to the allegations. Although we will not tell these people your identity unless you give consent, it is possible that the details of the report may lead them to believe that they know the identity of the Whistleblower.
- You should also be aware that it is possible for people to guess your identity if:
- you previously mentioned to other people that they are considering making a disclosure;
  - you are one of a very small number of people with access to the information; or
  - your disclosure relates to information that you have previously been told privately and in confidence.
29. Any breach of confidentiality will be treated as a serious matter and may be the subject of disciplinary action up to and including dismissal or termination of engagement with Defence Bank. Breaches of Whistleblower confidentiality are also an offence under the Corporations Act and the Taxation Administration Act and serious penalties apply for both individuals and corporations.
30. If you believe your confidentiality as a Whistleblower has been breached, you can make a complaint to one of the Nominated Officers listed in clause 15 or by contacting Your Call. You can also lodge a complaint with ASIC, APRA or the ATO.

#### **Protection against detrimental conduct.**

31. Defence Bank is committed to protecting the rights of Whistleblowers who have made Protected Reports and will not tolerate any detriment or threats of detriment against them or any other person (e.g. suspected whistleblowers or people who participate in investigations).
32. It is an offence under the *Corporations Act* and the *Taxation Administration Act* to cause, or threaten to cause, detriment to a person because they or someone else has made, may have made, proposes to make or could make a Protected Report and serious penalties apply for both individuals and corporations. A person who is subject to such detriment may also seek compensation or other remedies from a Court if they have suffered loss, damage or injury because of a Protected Report or because Defence Bank failed to take reasonable precautions and exercise due diligence to prevent the detriment.

- a. 'Detriment' includes dismissal, suspension, demotion, or termination of your employment or engagement with us; changes to your employment, position, or duties to your disadvantage; discrimination; harassment or intimidation; harm or injury (including psychological harm); damage to property, reputation, business or financial position; or any other damage.
- b. The following actions are not considered to be detriment:
  - i. reasonable administrative action taken to protect a Whistleblower from detriment (e.g. relocating them to another office to prevent victimisation);
  - ii. managing unsatisfactory work performance of a Whistleblower, in line with Defence Bank's usual performance management framework;
  - iii. Defence Bank will protect Whistleblowers from detriment arising from making a Protected Report by conducting a risk assessment of the disclosure to manage the risk of detriment to the Whistleblower:
    1. where applicable, making such reasonable adjustments as required to allow the Whistleblower to perform their duties at work without being potentially exposed to detriment (e.g. by changing reporting lines or location);
    2. implementing strategies to help the Whistleblower minimise and manage stress, time or performance impacts or other challenges resulting from the disclosure or its investigation;
    3. making available support services such as access to Defence Bank's independent Employee Assistance Program (EAP).

If you believe you have suffered detriment, you are encouraged to obtain independent legal advice in relation to your rights. You can make a complaint to one of the Nominated Officers listed in clause 15 or by contacting Your Call. You can also lodge a complaint with ASIC, APRA or the ATO.

### **Protection for Whistleblowers against litigation.**

33. If you make a Protected Report, you are protected from any of the following legal actions for doing so:
  - a. Civil liability (e.g. any legal action against you for breaching an employment contract, a duty of confidentiality or another contractual obligation);
  - b. Criminal liability (e.g. legal action against you for unlawfully releasing information, or other use of the Protected Report against you in a criminal proceeding (other than for making a false disclosure);
  - c. Administrative liability (e.g. disciplinary action for making the Protected Report).
34. You are still responsible for your own actions. These protections do not prevent action being taken against you for any Wrongdoing that you are involved in that is revealed in your report.

### **Other support available for Whistleblowers.**

35. We will support you while your Protected Report is being handled by Defence Bank.

36. If necessary, Defence Bank will appoint a Protection Officer to arrange or coordinate support and protection for Whistleblowers who have made or are in the process of making a Protected Report. A Whistleblower can contact Mano Simos, Chief Risk Officer (Whistleblower Protections Officer) to discuss how a Protection Officer may be able to provide support and protection.
- a. The role of the Protection Officer is to:
    - i. assess the immediate welfare and protection needs of a Whistleblower;
    - ii. safeguard the interests of a Whistleblower in accordance with this policy and the law; and
    - iii. address any issues or concerns of detriment.
  - b. Employees may also contact our Employee Assistance Program: Uprise on 1300 209 371.

### **How we handle Protected Reports.**

37. Any person who receives a Whistleblower report made under this policy must ensure that the report is managed in compliance with this policy and any relevant procedures. This is to ensure that the protections available for the Whistleblower are not compromised and that Defence Bank meets its legal obligations.

### **How do we investigate reports of Wrongdoing?**

38. Reports of alleged Wrongdoing made in accordance with this policy will be treated seriously and where appropriate will be thoroughly investigated by Defence Bank in accordance with this policy.
- a. After receiving a report about Wrongdoing, we will assess the information provided to determine whether it is a Protected Report, how it will be handled and whether an investigation is required. The precise steps to be taken to investigate a report will differ in individual cases but may include:
    - i. determination of the nature and scope of an investigation;
    - ii. appointment of an internal or external investigator (if it has been determined that an investigation is required) who is able to conduct the investigation in a fair, objective and independent manner;
    - iii. the investigator or other person asking the Whistleblower whether they consent to their identity being disclosed to investigate the report;
    - iv. interviewing the Whistleblower and any other relevant person to obtain information about the report;
    - v. determination of the nature of any technical, financial or legal advice that may be required to support the investigation;
    - vi. review of relevant documents and other information in relation to the report;
    - vii. the investigator making findings regarding the conduct reported.



39. Generally, if the Whistleblower can be contacted, we will confirm receipt of their disclosure within two business days. The investigation of a Protected Report will commence as soon as reasonably possible from the date we receive it. However, there may be reasons why an investigation may take longer. If we think there might be a delay with the investigation, we will tell the person who made the Protected Report (where possible).
40. Where possible and assuming that the identity of the Whistleblower is known, the Whistleblower will be kept informed of when the investigation process has begun, while the investigation is in progress and after the investigation has been finalised, subject to confidentiality and privacy considerations.
41. Defence Bank may decide to take action in response to any findings which may include, but is not limited to, disciplinary action, reporting the matter to an appropriate regulator, conducting training or addressing procedural and policy deficiencies.

#### **Treatment of employees who are the subject of a Whistleblower report.**

42. Defence Bank will take all reasonable steps to ensure that any employee who is the subject of a Protected Report is afforded fair treatment and an impartial investigation in accordance with this policy. Generally, when an investigation is conducted, employees who are the subject of a Protected Report may be, within the constraints of confidentiality:
  - a. told about the substance of the allegations;
  - b. given a fair and reasonable opportunity to respond to the allegations before the investigation is finalised; and
  - c. informed about the findings of the investigation and given an opportunity to respond to those conclusions before any action is taken against them (subject to legal, privacy and confidentiality requirements).
43. Before providing any information to an employee who is the subject of a Protected Report we will:
  - a. make sure the information does not include your identity;
  - b. make sure we have taken all reasonable steps to reduce the risk that you will be identified from the information; and
  - c. only provide information that is reasonably necessary for investigating the issues raised in the Protected Report.
44. Employees who are the subject of a Protected Report may access Defence Bank's independent Employee Assistance Program (EAP) for additional support.

#### **Internal reviews.**

45. If you make a Protected Report, or you are the subject of a Protected Report, and you are not satisfied with the outcome, you may ask for an internal review of our decision.
46. Internal reviews will be directed to the CEO or Chair of the Board, or an alternative Nominated Officer if there is a conflict.
47. We may refuse to conduct an internal review if no new information is available or if the new information would not change the outcome.

48. If you are not satisfied with our response, you may lodge a report or complaint with ASIC, APRA or the ATO in accordance with the law.

## Reporting to the Board.

49. The Board (through the Risk and Compliance Committee) will be provided with confidential reports on the number and type of whistleblowing incidents quarterly to enable it to address any issues at a regional or group level. Reports will be on a 'no names' basis to maintain the confidentiality of matters raised under this policy.
50. The Board will monitor the whistleblower management system to ensure that the broader trends, themes and/or emerging risks highlighted by the disclosures made under this policy are addressed and mitigated as part of Defence Bank's risk management and corporate governance.

## Review, Access and Training in relation to this policy.

51. This policy will be available to officers and employees of Defence Bank on the intranet. A copy will also be available on our website to ensure it is accessible for all eligible whistleblowers.
52. This policy may be reviewed and amended from time to time and will be reviewed by Defence Bank at least every three years.
53. The Chief People Officer will be responsible for conducting upfront and ongoing education and training on the whistleblower policy, processes and procedures to all officers and employees.

## Roles and responsibilities.

54. The roles and responsibilities under this Policy are set out in the table below:

| Position.                                  | Responsibilities.  |
|--|--|
| <b>Board (Policy approver)</b>             | <p>Approving or rejecting any material changes to this Policy, making sure it is adequate and appropriate.</p> <p>If appropriate, advising the Document Owner to make any amendments that the Board thinks are necessary.</p>  |
| <b>Chief People Officer (Policy Owner)</b> | <p>Making sure this Policy meets the requirements of the Policy Framework.</p> <p>Reviewing this Policy at least triennially and if ever things change so that it should be reviewed earlier.</p> <p>Monitoring the environment and any exemptions to this Policy, and making sure this Policy stays relevant and up-to-date.</p> <p>Agreeing with the Board how often this Policy must be reviewed and making sure it is reviewed at least triennially.</p> <p>Approving any non-material changes to this Policy (e.g. a change to the Key Contact).</p> <p>Making sure that any changes to this Policy are well communicated (including to regulators if required) and that everyone who needs to follow this Policy understands the changes.</p> <p>Giving assurance to the Board at least annually that this Policy is adequate and effective.</p> |

| Position.                                    | Responsibilities.   |
|--|---|
|  | <p>If appropriate, telling the Policy Owner to make any amendments that the Board thinks are necessary.</p> <p>Oversight of Whistleblowing Program.</p>   |
| <b>Directors, employees and contractors.</b> | Following this Policy and being guided by it.   |
| <b>Chief People Officer (Key contact)</b>    | Helping the Chief Executive Officer and the Board meet their responsibilities by interpreting the Policy, providing training and expert advice, and answering questions about the Policy.                                       |
| <b>Managers</b>                              | Ensuring that employees are aware of this policy and how to make Protected Reports; Not cause detriment to a Whistleblower in relation to making, or considering to make, a Protected Report.                                   |
| <b>Whistleblower Investigation Officer</b>   | Conducting an initial assessment of the disclosure to determine whether it is a Protected Report and how it should be investigated, including appointment of an independent, external investigator where required.              |
| <b>Whistleblower Protection Officer</b>      | Appointed by a Nominated Officer if requested by a Whistleblower. Work with the Whistleblower to understand and manage welfare concerns arising from making a Protected Report, and help support a supportive work environment. |

## Breaches.

55. If you breach this Policy, Defence Bank may take disciplinary action against you. This will depend on the circumstances, including if your breach is deliberate, how severe it is and if there have been previous occurrences. Disciplinary action could include a warning, dismissal, or Defence Bank ending its business relationship with you.
56. If you break the law you might face criminal or civil liability.
57. If you become aware of a breach of this Policy, advise the Chief People Officer.

## Contacts for questions and more information.

This Policy is owned by the Chief People Officer. If you have any questions or would like more information about this Policy, you should contact the Chief People Officer.

## Document information.

|                                 |  |
|---------------------------------|--|
| <b>Effective from</b>           | 24 July 2023   |
| <b>Owner</b>                    | Chief People Officer   |
| <b>Approver</b>                 | Board  |
| <b>Next review due</b>          | July 2026  |
| <b>Entities this applies to</b> | Defence Bank Limited, its subsidiaries and any other entity or joint venture which it controls (collectively <b>Defence Bank</b> ) except those which have been given exemption as shown below.  |
| <b>Exemptions</b>               | N/A  |
| <b>Related documents</b>        | <p>Key documents that should be read in conjunction with this Policy:</p> <ul style="list-style-type: none"> <li>• People Operational Policy;</li> <li>• Defence Bank Process - Speak Up reporting process;</li> <li>• <i>Corporations Act 2001</i> (Cth);</li> <li>• <i>Taxation Administration Act 1953</i>; and</li> <li>• ASIC Regulatory Guide 270 - Whistleblower policies.</li> </ul> |

## Document history.

| Version. | Date.      | Amended by.          | Details of amendment.  |
|----------|------------|----------------------|--|
| 1.0.     | 24/07/2023 | Chief People Officer | New standalone policy to replace Policy 8, section 3.            |
| 1.1      | 17/10/2023 | Chief People Officer | Review cycle updated from 2 to 3 years. And CDIO update to CTDO. |
| 1.2      | 31/10/2023 | Chief People Officer | All clause cross references updated as they were incorrect.      |
| 1.3      | 21/11/2023 | Chief People Officer | Clause 11.c.i updated to reflect correct year.                   |
| 1.4      | 30/06/2024 | Chief People Officer | Clause 12.e updated to add Modern Slavery                        |



## Appendix 1.

### Who can a Protected Report be made to?

The following individuals and organisations can receive Protected Reports:

- A Nominated Officer, as specified in clause 15.
- Defence Bank's external whistleblowing service, Your Call, as specified in clause 16.
- A director or officer of Defence Bank or one of the following executive managers:
  - Chief Executive Officer
  - Chief People Officer
  - Chief Risk Officer
  - Chief Financial Officer
  - Chief Marketing & Product Officer
  - Chief Member & Growth Officer
  - Chief Digital & Technology Officer
  - Another senior manager of Defence Bank who makes, or participates in making decisions that affect the whole, or a substantial part, of the business of Defence Bank or who has the capacity to significantly affect its financial standing.
- In accordance with the *Corporations Act*, a whistleblowing report may also be made externally to one of the following:
  - A legal practitioner for the purposes of obtaining legal advice or legal representation about the operation of the whistleblower provisions in the Corporations Act;
  - ASIC, APRA or a Commonwealth authority prescribed under the Corporations Act (see ASIC [Information Sheet 239](#) *How ASIC handles whistleblower reports* for more information);
  - An actuary, auditor or member of an audit team conducting an audit of Defence Bank.
- A report under the Taxation Administration Act may also be made externally to:
  - A legal practitioner for the purposes of obtaining legal advice or legal representation;
  - The Commissioner for Taxation;
  - A registered tax agent or BAS agent who provides tax agent services to Defence Bank; or
  - An auditor or member of the audit team conducting an audit of Defence Bank.

### Public interest disclosures.

You may make a disclosure in the public interest to a member of parliament or a journalist if:

- you have previously made that disclosure to ASIC, APRA or another Commonwealth body prescribed by regulation; and

- at least 90 days have passed since the disclosure was made and you do not have reasonable grounds to believe that action is being, or has been, taken to address the misconduct to which the previous disclosure related; and
- you have reasonable grounds to believe that making a further disclosure of the misconduct would be in the public interest; and
- after the end of the 90-day period you notify the body to whom you made the disclosure (ASIC, APRA or other Commonwealth body) in writing with sufficient information to identify the previous disclosure, and state that you intend to make a public interest disclosure to a member of parliament or a journalist; and
- the extent of the information disclosed in the public interest disclosure is no greater than is necessary to inform the recipient of the misconduct or the improper state of affairs or circumstances.

### **Emergency disclosures.**

You may make an emergency disclosure to a member of parliament or a journalist if:

- you previously made that disclosure to ASIC, APRA or another Commonwealth body prescribed by regulation;
- you have reasonable grounds to believe that the information concerns a substantial and imminent danger to the health or safety of one or more persons or to the natural environment;
- you notify the body to whom you made the disclosure (ASIC, APRA or other Commonwealth body) in writing with sufficient information to identify the previous disclosure, and state that you intend to make an emergency disclosure to a member of parliament or a journalist;
- the extent of the information disclosed in the emergency disclosure is no greater than is necessary to inform the recipient of the substantial and imminent danger.

It is important to understand that a report may only be made to a journalist or a parliamentarian in the circumstances described above. You should seek independent legal advice before making a public interest disclosure or an emergency disclosure to a member of parliament or a journalist.

### **Personal work-related grievances.**

Clause 13 sets out what can be reported as Wrongdoing under this policy and in accordance with Australian whistleblowing protection laws. In some circumstances, a personal work-related grievance may be a protected disclosure if, in summary:

- it includes information about Wrongdoing or information about a personal work-related grievance or is bundled with a report of Wrongdoing (mixed report);
- it relates to a breach by Defence Bank of employment or other specified laws punishable by imprisonment of 12 months or more;
- it includes information about Wrongdoing beyond an individual's personal circumstances, demonstrates a systemic issue within Defence Bank, has significant implications for Defence Bank or indicates that Defence Bank has engaged in conduct that represents a danger to the public;



- concerns detriment to a person because they have or may be considering reporting Wrongdoing; or
- it is made to a legal practitioner for the purposes of obtaining advice or legal representation in relation to the operation of the law about whistleblowers.