Australian Government

Northern Australia Infrastructure Facility

Incident Reporting Policy

February 2019

www.naif.gov.au

Contents

1. Definitions 3
2. What is an Incident 3
   2.1 Data Breaches 4
3 Statement of Commitment 4
4 Reporting an Incident 4
5 Protections Provided to the Reporting Person 6
   5.1 Confidentiality 6
   5.2 Other protections 6
6 Responsibilities 6
   6.1 Board Responsibilities 6
   6.2 Chair of the Board's Responsibilities 6
   6.3 Chair of the Board Audit and Risk Committee's Responsibilities 6
   6.4 CEO's Responsibilities 7
   6.5 Staff Responsibilities 7
7 Review and Approval 7
8 Seeking Assistance 7
Appendix A 8

1. Definitions

The following definitions apply when used in this Policy:

CEO means NAIF's Chief Executive Officer

Data Breach occurs when personal information (as defined in section 6 of the Privacy Act) held or controlled by NAIF is lost or subjected to unauthorised access, modification, use or disclosure or other misuse or interference.

Disclosable Conduct means conduct that:

- contravenes the law;
- is corrupt;
- perverts the course of justice;
- results in wastage of public funds;
- is an abuse of public trust;
- unreasonably endangers health and safety or endangers the environment;
- is maladministration, including conduct that is unjust, oppressive or negligent; or
- conduct by a public official that, if proved, would give rise to disciplinary conduct against the official;

but

- excludes government policy, action or expenditure with which a person disagrees.

Incident means any of the events set out in section 2 of this Policy.

PID Policy means the Public Interest Disclosure Policy.

Privacy Officer is the Manager, Risk & Compliance or another member of Staff as appointed by the CEO from time to time.

Public Interest Disclosure means a disclosure made under the PID Policy about Disclosable Conduct by an agency, a public official or a contracted Commonwealth service provider (in connection with the contract).

Recipient, in relation to a report made under this Policy, means the CEO, the Chair of the Board or the Chair of the Board Audit and Risk Committee.

Reporting Person means a member of Staff who reports an Incident.

Staff means persons employed by, or operating under an employment or similar contract with NAIF including full-time and part-time Staff, consultants, contractors and Efic personnel under a Service Level Agreement.

2. What is an Incident

An Incident is defined as a past, present or likely future breach, or a suspicion of a breach, by any party of a law or NAIF policy and includes:

- a corrupt practice, including offering, or giving, or accepting, a benefit directly or indirectly as a result of that corrupt practice;
- a fraudulent practice being any act or omission by a party, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead another party, to obtain for the first party or a third party a benefit to which that party would not otherwise be entitled;
- a coercive practice being any attempt by a party to influence improperly the actions of another party, including through the use of threats of harm or disadvantageous treatment;
- a collusive practice being an arrangement between two or more parties designed to achieve an improper purpose, including improperly influencing the actions of another party;
- theft or improper use of NAIF's or a service provider's assets;
- a conflict of interest which has not been properly managed and disclosed, being any situation in which a party has an interest that could influence that party's performance of their responsibilities or compliance with applicable laws and regulations (and related rules) or results in the party obtaining a benefit to which they would not otherwise be entitled; or
- an external allegation or report of any of the matters referred to above.

2.1 Data Breaches

NAIF's Data Breach Response Plan (**Response Plan**) sets out the procedure and lines of authority to be followed by Staff in the event that NAIF experiences a data breach, or suspects that a data breach may have occurred.

Under Part IIIC of the *Privacy Act 1988* (**Privacy Act**), NAIF is required to notify the Privacy Commissioner and affected individuals of eligible data breaches. The Response Plan details how NAIF can comply with its Privacy Act obligations.

All Staff have a responsibility to:

- protect personal information from misuse, interference and loss and unauthorised access, modification or disclosure;
- be alert to possible data breaches;
- respond quickly to contain possible data breaches and escalate them to their manager or directly to the Privacy Officer, and
- provide any further assistance required to investigate, respond to privacy data breaches and prevent future incidents.

There are also specific responsibilities for the Privacy Officer and other team members where required to investigate and manage NAIF's response to eligible data breaches.

3 Statement of Commitment

NAIF is committed to the following key elements of this Policy:

- Staff are strongly encouraged to make a Public Interest Disclosure under the PID Policy where they become aware of an Incident that is covered by the Public Interest Disclosure Act;
- Staff are strongly encouraged to make a report under this Policy if they become aware of an Incident that is not covered by the Public Interest Disclosure Act – this would usually be because the conduct in question was carried out by a person who was not a public official;
- a Reporting Person will not be subject to any discrimination, harassment or prejudice, to themselves, their colleagues or relatives because they have made a report under this Policy; and
- remedial action in response to Incidents will be taken where appropriate and will be communicated to Staff.

4 Reporting an Incident

Staff should report Disclosable Conduct as a Public Interest Disclosure under the PID Policy. The PID Policy is a policy that has been developed to meet NAIF's obligations under the *Public Interest Disclosure Act 2013* (PID Act). Under the PID Policy Staff can report any matter that appears to be Disclosable Conduct to their supervisor or to an authorised officer in NAIF, including the CEO. Staff who make a public interest disclosure under the PID Policy will generally have the protections of the PID Act.

However, there are circumstances where Staff may not be able to make a report under the PID Policy. For example, a Staff member may encounter an issue, or receive a report about an issue, that is not Disclosable Conduct as defined in the PID Act. This would typically be because the conduct in question was carried out by a person who was not a 'public official' within the meaning of the PID Act. Where an Incident is of this nature, it should be reported under this Policy, although staff should note that the protections under the PID Act will not apply.

A report under this Policy can be made to the CEO, or to the Chair of the Board or to the Chair of the Board Audit and Risk Committee.

The Recipient of a report under this Policy must consider whether to investigate the report. The Recipient must investigate a report from a Reporting Person, unless the Recipient reasonably determines that:

- the information does not, to any extent, concern an Incident;
- the report is frivolous or vexatious;
- the information is the same, or substantially the same, as information which has been, or is being, investigated under:
    - this Policy;
    - a law of the Commonwealth; or
    - the executive power of the Commonwealth;

  and it would be inappropriate to conduct another investigation at the same time and the Recipient is reasonably satisfied that there are no further matters concerning the Incident that warrant investigation;
- the Reporting Person has informed the Recipient that the Reporting Person does not want the investigation of the Incident to be pursued, and the Recipient is reasonably satisfied that there are no matters concerning the Incident that warrant investigation; or
- it is impractical for the Incident to be investigated because:
    - the Reporting Person is anonymous and is not contactable;
    - the Reporting Person refuses or fails, or is unable, to give, for the purposes of the investigation, such information or assistance as the person who is, or will be, conducting the investigation requires the Reporting Person to give; or
    - of the age of the information provided by the Reporting Person.

If the Recipient decides to investigate the report, they may investigate as they see fit and may appoint an independent person to investigate or advise on the matter.

In responding to an Incident from a Reporting Person, the Recipient will:

- if possible, acknowledge receipt of the disclosure by the Reporting Person;
- assess the risks of reprisal against a Reporting Person in accordance with this Policy;
- provide a secure and confidential environment to obtain information from the Reporting Person in relation to the Incident;
- subject to any legal and regulatory requirements, comply with the confidentiality requirements contained in this Policy to the extent possible;
- where appropriate, arrange for an independent person to conduct an investigation;
- arrange for the investigation to be conducted with honesty, integrity, professionalism and efficiency and to comply with all applicable Australian laws;
- maintain all records relating to the investigation in a secure manner;
- provide a method for investigating the Incident that will not subject the Reporting Person or any other Staff to discrimination, harassment or prejudice;
- should it become necessary to disclose the identity of the Reporting Person in accordance with this Policy, discuss this with the Reporting Person first;
- if the investigation concludes that there is credible evidence that an offence may have occurred decide whether to refer the matter to the Australian Federal Police or other appropriate law enforcement agencies;
- where the recipient is not the CEO – to advise the CEO of remedial action to be taken by NAIF in respect of the Incident; and
- provide the Reporting Person with feedback regarding actions taken in response to the Incident. The extent to which the Reporting Person will be informed of specific actions will vary, depending on the nature of the Incident.

A diagram of the actions to be taken in response to a report under this Policy is set out in Appendix A to this Policy.

5 Protections Provided to the Reporting Person

5.1 Confidentiality

A Recipient will make every reasonable effort to protect the Reporting Person's identity. However, the Reporting Person's identity, or information that would effectively identify them, may need to be disclosed to certain other people if that is necessary:

- to investigate the disclosure effectively ;
- to protect them against reprisals (for example, if there are concerns that it is impossible for them to remain in their current workplace); or
- because of a requirement of law, including procedural fairness.

If it is necessary or highly likely that the discloser's identity will be revealed, the Recipient will discuss this with the Reporting Person before proceeding.

The Recipient must keep secure and confidential the records of a report and how and when a report was made under this Policy. Each report should be given a unique reference number. Details of the risk assessment of reprisal, any investigation, notification to the Reporting Person and others will also be kept. The Recipient and any other person undertaking an investigation must also keep records of their investigation secure and confidential. Any breach of confidentiality of the information provided by a Reporting Person, or a Reporting Person's identity, will be subject to a separate investigation and, if a member of Staff who is an employee of NAIF is found to have disclosed the information, disciplinary action may be taken including termination of employment.

5.2 Other protections

NAIF does not tolerate reprisal action related to an Incident reported by a Reporting Person, such as discrimination, harassment or prejudice toward a Reporting Person. If a member of Staff who is an employee of NAIF is found to have taken reprisal action against a Reporting Person, disciplinary action may be taken, including termination of employment.

As soon as possible after a report of an Incident from a Reporting Person is received, the Recipient must assess the risk that reprisal may be taken against that Reporting Person. If a Reporting Person wishes their identity to remain anonymous, the Recipient must conduct a risk assessment as soon as possible after the report is made.

The Recipient, where appropriate, will plan and implement strategies to control the risks of reprisals or related workplace conflict. Where possible, the Reporting Person will be consulted before any decision is made.

The risk assessment should be monitored and reviewed by the Recipient as necessary including by checking with the Reporting Person to see if reprisals have been made or threatened.

6 Responsibilities

6.1 Board Responsibilities

The Board is responsible for approving this Policy.

6.2 Chair of the Board's Responsibilities

The Chair of the Board is responsible for receiving and responding to reports made to them as a Recipient under this Policy.

6.3 Chair of the Board Audit and Risk Committee's Responsibilities

The Chair of the Board Audit and Risk Committee is responsible for receiving and responding to reports made to them as a Recipient under this Policy.

6.4 CEO's Responsibilities

The CEO is responsible for:

- receiving and responding to reports made to them as a Recipient under this Policy;
- promoting a culture of prompt reporting of circumstances that may constitute an Incident;
- arranging for Staff to receive periodic training on this Policy;
- allocating the appropriate resources to implement the management of Incidents under this Policy;
- implementing appropriate remedial action for Incidents; and
- ensuring that consequences of any breach of this Policy are communicated to Staff.

6.5 Staff Responsibilities

Staff are expected to report any Incident that comes to their attention, either under the PID Policy or this Policy, as applicable.

7 Review and Approval

This Policy will be reviewed annually, or more frequently if required, by or on behalf of the NAIF Executive, to ensure it remains aligned with governing legislation and best practice. The Board approves all material amendments and reviews the Policy at least every two years.

The Manager, Risk & Compliance will ensure material changes to this Policy are communicated to Staff in a timely manner.

8 Seeking Assistance

If Staff have any queries in relation this Policy, they should discuss them with the CEO.

Appendix A

Diagram of actions to be taken in respect of a report made under this Policy