1 Purpose

In carrying out diverse functions and activities, Taronga Conservation Society Australia ('Taronga') creates, stores and collects information, including the personal and health information of others (eg employees, guests, students and donors) and other classified or sensitive information. This data is held and managed in line with the *Privacy and Personal Information Protection Act 1998* ('PPIP Act'), the *Health Records and Information Privacy Act 2002* ('HRIP Act'), the *State Records Act 1998* and relevant Taronga policies, including the Privacy Management Plan and Cyber Security Policy.

This Data Breach Policy sets out Taronga's strategies to prevent, prepare for and manage all data breaches. The Policy outlines steps for the mandatory notification and reporting of 'eligible data breaches' under Part 6A of the PPIP Act - the Mandatory Notification of Data Breach (MNDB) Scheme. 'Eligible data breaches' are those involving unauthorised access or disclosure of personal or health information that could cause serious harm to persons affected by the breach.

2 Scope

This Policy applies to Taronga's employees, volunteers, contractors and staff of contracted bodies who are engaged to perform Taronga's functions.

This Policy also applies to Taronga Board and Committee members.

The Policy applies to third party service providers who hold personal or health information on behalf of Taronga.

This Policy applies to all instances of unauthorised access or unauthorised disclosure of Taronga information. The Policy sets out mandatory procedures for managing 'eligible data breaches' and guides voluntary action for other data breaches.

3 Definitions

In this Policy:

Term	**Definition**
Data breach	A data breach occurs when information held by Taronga is subject to unauthorised access, unauthorised disclosure, or is lost in circumstances where the loss is likely to result in unauthorised access or disclosure. A data breach may be accidental or malicious. It may involve information in digital or hard copy. A breach may occur internally within Taronga, between Taronga and other organisations, or by an external person or entity accessing Taronga's data without authorisation. Examples include: • Accidental loss or theft of data or equipment on which such data is stored (eg loss laptop, mobile phone, USB stick or paper file) • Unauthorised use, access to or modification of data or information systems (eg sharing of user login details (deliberately or accidentally) to

	enable unauthorised access or make unauthorised changes to data or information systems, accidental grant of access to sensitive records) • Unauthorised access / hacking by external body affecting Taronga systems or the systems of a third party that holds Taronga's data • Unauthorised disclosure of classified material or personal information (eg email sent to an incorrect recipient) • Disclosure of user login details through phishing • Malware infection or ransomware attacks • Disruption to or denial of IT services
Eligible data breach ('EDB') ***And*** ***'Affected individual'***	Eligible data breach ('EDB') is defined in Part 6A of the PPIP Act. An eligible data breach occurs where: 1. (a) There is unauthorised access to, or unauthorised disclosure of, personal or health information held by Taronga, or (b) Personal or health information held by Taronga is lost in circumstances where unauthorised access or disclosure is likely, and 2. The likely or actual unauthorised access or disclosure is likely to result in serious harm to the individual to whom the information relates ('affected individual').
Personal information	Personal information has the same meaning as defined in s 4 PPIP Act, that is: information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. There are exceptions that apply, including information that is contained in a publicly available publication, or information about persons who have been dead for more than 30 years. (See further: Taronga's Privacy Management Plan)
Health information	Health information has the same meaning as defined in s 6 of the HRIP Act, that is, information or an opinion about a person's physical or mental health, disability or information related to the provision of a health service. (See further: Taronga's Privacy Management Plan)
Held by Taronga	'Held' has the meaning as defined in Part 6A of the PPIP Act: Information is held by Taronga if: (a) Taronga is in possession or control of the information, or (b) Information is contained in a State record for which Taronga is responsible under the *State Records Act 1998*.

Assessor	'Assessor' in this Policy, is the person from time to time directed by the Chief Executive to assess a data breach under s 59 G of the PPIP Act.
Chief Executive ('CE')	The Chief Executive of Taronga Conservation Society Australia, (who is the head of Taronga under Pt 6A of the PPIP Act), and includes any person acting in the role, and delegates as nominated in this Policy or by separate instrument

4 Identifying and reporting data breaches

Taronga's people may become aware of a data breach through a number of ways, including:

- Personal knowledge (eg realisation that USB stick is lost)
- Internal communication with a staff member or contractor (eg advising that email sent to incorrect recipient)
- Contact from members of the public (eg via phone or email to specific officers, or generic Taronga / privacy inbox).

Taronga's people must report **all data breaches** or possible data breaches immediately to the IT Service Desk through Taronga's JIRA system. The Information Management Specialist will monitor and manage these reports, in consultation with the Manager, Governance and Risk.

Phishing attempts or suspected phishing emails are to be reported through the Outlook 'Report Message' tab.

Prompt reporting is essential to give Taronga the best chance to contain the breach, mitigate against any potential harm and ensure any legislated response timeframes are met.

5 Responding to a data breach

5.1 Overview

This Policy sets out how Taronga responds to a data breach, following six key steps:

1. Initial assessment / triage
2. Contain breach
3. Assess breach and mitigate harm
4. Notify Privacy Commissioner
5. Notify affected persons
6. Post incident review

See **Appendix A**: Data Breach Assessment Flow Chart for a summary of the assessment process and delegates.

See further: A guide to managing data breaches in accordance with the PPIP Act, IPC June 2023

5.2 Initial assessment and triage

5.2.1 Immediate containment and harm mitigation actions

Upon receiving a report of a data breach, the Information Management Specialist will work with the reporter to take steps to contain the breach and mitigate harm resulting from the breach (see Section 5.4).

Immediate actions to contain the breach may include:

- Recalling emails (but note action is not effective to contain the breach if the email has already been opened)
- Inactivating attachment links on emails, if possible
- Changing passwords or system IT access controls

5.2.2 Initial assessment

The Information Management Specialist, in consultation with the Manager, Governance and Risk, will conduct an initial assessment of the breach, considering factors relevant to the assessment (see Section 5.6.3). Relevant factors include:

- Whether the data includes or may include personal or health information and the types of information
- Whether the data is otherwise sensitive or classified
- Who is affected by the breach, the number of people affected, or agencies / third parties affected
- Likelihood of serious harm to affected individuals
- Efficacy of containment actions taken

5.2.3 Possible EDB escalated to CE

If the Information Management Specialist considers that the data breach is, or could reasonably be an eligible data breach, the breach is escalated to the Chief Executive ('CE') (or delegate).

The CE will continue action to contain the breach and mitigate harm resulting from the breach.

The CE will direct an assessment and, if a breach is assessed as an eligible data breach, fulfil notification and reporting requirements (see Sections 5.6, 5.7 and 5.8)

5.2.4 Initial assessment - data breach not EDB

If the data breach does not involve personal or health information or is otherwise not considered an 'eligible data breach', the MNDB Scheme (Sections 5.6, 5.7 and 5.8) does not apply to the breach.

However, for these breaches, Taronga will still be guided by this Policy in its response to the breach.

In particular, Taronga will:

- Contain the breach (Section 5.4)

- Mitigate harm arising from the breach (Section 5.5)
- Convene response teams and implement specific response plans, if necessary (Section 5.3)
- Consider voluntary notification to persons affected by the breach (Section 5.8)
- Notify relevant bodies as required (eg insurer, Police, State Records, NSW Cyber Security Centre), (Section 5.10)
- Conduct post incident review and implement improvement and prevention actions (Section 5.11)

5.3 Response Teams

5.3.1 Data Breach Response Team

The CE may convene a Data Breach Response Team to coordinate, advise and implement actions in response to a data breach. The Data Breach Response Team acts within normal business operations to support Taronga's response to a data breach.

The Data Breach Response Team may be convened where the initial assessment of the breach suggests:

- A high risk of serious harm to persons affected by the breach including physical safety, financial and reputational harm, considering the type and sensitivity of data, number of persons affected and other relevant factors (see Section 5.6.3)
- A high risk to Taronga operations or reputation, regardless of whether the breach is an EDB
- A complexity of factors and actions that would benefit from a coordinated approach and multidisciplinary advice and assistance

5.3.2 Data Breach Response Team - membership

Taronga's Data Breach Response Team is made up of one or more of the following roles (the Core team):

- Divisional Director, Corporate Services and Governance
- Divisional Director, Marketing, Communications and Fundraising
- Divisional Director, People, Culture and Safety
- Director, IT
- Manager, Governance and Risk
- Manager, Media and Communications
- CRM Platform Manager
- Other Executive nominated by Chief Executive

AND

- Any subject matter expert from the area of the data breach, as nominated by a member of the Core team

The Divisional Director, Corporate Services and Governance is the Chair of the Data Breach Response Team.

If the Divisional Director, Corporate Services and Governance is not available, the sitting members decide on membership of the DBRT and the Chair.

5.3.3 Role of Data Breach Response Team

The responsibilities of the Data Breach Response Team are as follows:

- Decide on membership and nominate Chair (if Divisional Director Corporate Services and Governance is not available)
- Direct, oversee and advise on immediate actions to contain the breach and mitigate any loss or harm caused by the breach
- Assist decision makers in the assessment process by gathering information, providing subject matter expertise, providing recommendations and advice regarding actions including appointment of suitable Assessor
- Advise on the application of exemptions from requirement to notify affected individuals
- Coordinate and advise on notification actions under the Policy
- Participate in post incident reviews

5.3.4 Business Continuity and Crisis Management

If the data breach represents a business disruption event, that cannot suitably be managed within normal business operations, the CE may activate Taronga's crisis management plan as the overarching framework for action under this Policy.

5.4 Contain breach

Following the initial assessment and immediate containment actions, the CE will continue to prioritise actions to contain a data breach and minimise any possible damage arising from the breach.

Possible actions to contain the breach include:

- Stop an unauthorised practice or access
- Recover the personal or health information (and ensuring no copies have been made by a third party)
- Shut down the system that has been breached
- Suspend the business activity that resulted in the breach
- Revoke or change access codes or passwords

5.5 Mitigate harm

The CE will prioritise action to mitigate the risks of harm arising from the data breach. Actions to mitigate harm will commence immediately after becoming aware of the breach and continue throughout the assessment and response process.

Actions to mitigate harm caused by a data breach include:

- Acting swiftly to contain the breach

- Developing communications and notifying affected individuals as soon as possible to allow protective action to take place
- Providing supports to affected individuals (eg dedicated helpline or specialist cyber security advice)
- Taking action to limit dissemination of published information (eg seeking removal from public websites)
- Taking a precautionary approach to assessing the nature of the breach and type of information likely to be affected

5.6 Assess breach

5.6.1 Assessment of data breach

If a data breach is initially assessed as a possible eligible data breach, the CE will refer the breach to an appropriate Assessor, having regard to the nature of the breach and relevant circumstances.

Assessors may be an officer or employee of Taronga, an officer or employee of another agency acting on Taronga's behalf, or a person engaged by Taronga to carry out the assessment.

The Assessor must not have been involved in actions or omissions that led to the data breach.

The role of the Assessor is to:

- Gather information regarding the breach – contact relevant stakeholders and make investigations (eg through data logs and other evidence) as to what information is, or may have been compromised and the nature of the breach.
- Analyse – review the information collected above and evaluate the scale, scope and content of the suspected data breach and the potential for affected individuals to be likely to suffer serious harm as a result of the breach.
- Assess – decide whether the data breach is an EDB – whether it is likely to result in serious harm to affected persons.

5.6.2 Assessment to be completed within 30 days

The assessment must be carried out as soon as possible, and within 30 days of Taronga becoming aware that an eligible data breach may have occurred.

The CE may approve an extension of time to complete the assessment if, in the view of the CE, it is not reasonably possible for the assessment to be completed within 30 days.

If an extension has been approved, Taronga will, within the 30 day time period:

- Commence the assessment
- Notify the Privacy Commissioner in writing that the assessment has commenced, that an extension has been approved, brief reasons for the extension and the length of the extension period

If the assessment is not completed in the extension period, Taronga will notify the Privacy Commissioner before the end of the extension period of the progress of the assessment and revised extension period.

Taronga will continue to mitigate the harm caused by the breach, throughout the assessment and response process, (see Section 5.5)

5.6.3 Assessment – factors to consider

The Assessor, in deciding whether a data breach could result in serious harm (and therefore be an EDB), assesses whether the data breach will or may result in a real and substantial detrimental effect to the individual.

The Assessor considers the individual circumstances of each case, and all relevant factors including:

- The types of personal or health information involved and the combination of affected data types - financial information, combination of identify information, health information present a higher risk for serious harm.
- The sensitivity of the breached data – health information and sensitive information as set out in s 19 PPIP Act such as racial, political and religious information present a higher risk for serious harm.
- The amount of time information has been exposed or accessible prior to detection of the breach – longer exposure times present a higher risk for likelihood of unauthorised access and potential serious harm.
- If known, the circumstances of the individuals affected, and any particular vulnerabilities – the circumstances of some affected individuals may present a higher risk of serious harm, for example people impacted by family violence, public figures, young age.
- The presence and effectiveness of any security measures in place to protect the data – effective security controls such as encryption and MFA will suggest a lower risk of unauthorised access and resultant serious harm.
- Mitigation actions taken to reduce harm following the breach – swift, effective action taken to recover the data and contain the breach leads to a lower risk of unauthorised access and resultant serious harm.
- The circumstances of the breach, including the persons who have unauthorised access to the data, and their likely intentions or motivations – personal information obtained through a cyber attack by a malicious actor suggests a higher risk for serious harm.
- The nature of harm that has occurred or is likely to occur – harm may be physical, psychological, financial, reputational, identity theft or fraud.
- The ease with which information can be accessed and individuals identified – breached information that is easily matched in itself or with reference to other publicly available information presents a greater risk for serious harm.
- The number of people affected – the higher the number of affected persons, the more likely it is that a proportion of those affected persons may suffer serious harm, for various reasons, as a result of the breach.

Sometimes the nature of the access or disclosure is unclear or unable to be ascertained. In these cases, the Assessor is to take a precautionary approach when assessing the data breach, and consider the totality of any compromised data, rather than known access / disclosure of data.

The Assessor must have regard to the IPC Guidelines – Guidelines on the assessment of data breaches under Part 6A of the PPIP Act, IPC, September 2023.

5.6.4 Assessor advises CE of outcome of assessment

The Assessor advises the CE of the outcome of the assessment: whether, in the Assessor's view, the data breach is an EDB, or there are reasonable grounds to believe the data breach is an EDB.

5.6.5 CE decides if breach is eligible data breach

The CE reviews the assessment and decides whether:

- The data breach is an EDB, or
- There are reasonable grounds to believe the data breach is an EDB

If the CE decides the breach is an EDB, or has reasonable grounds for so believing, Taronga must report the breach to the NSW Privacy Commissioner and notify affected individuals (if no exemption applies) (see Sections 5.7 and 5.8).

If the CE decides there is **no** eligible data breach, notification to the Privacy Commissioner and affected persons is not required. However, Taronga will still be guided by this Policy in responding to the breach.

In particular, Taronga will:

- Continue containment measures (Section 5.4)
- Continue harm mitigation measures (Section 5.5)
- Convene response teams and implement specific response plans, if necessary (Section 5.3)
- Consider voluntary notification to persons affected by the breach (Section 5.8)
- Notify relevant bodies as required (eg insurer, Police, State Records, NSW Cyber Security Centre), (Section 5.10)
- Conduct post incident review and implement improvement and prevention actions (Section 5.11)

5.7 Notification of EDB to Privacy Commissioner

The CE must immediately notify the Privacy Commissioner of an eligible data breach, providing as much information as reasonably practicable as requested in the approved form – Data Breach Notification to Privacy Commissioner.

If information requested in the approved form is not available at the time of notification, Taronga will notify the Privacy Commissioner of any further information after notification of affected individuals (see Section 5.8), or if an exemption applies (see Section 5.9), as soon as practicable after that decision.

5.8 Notification of EDB to affected individuals

If the CE decides there has been an eligible data breach, and the Privacy Commissioner has been notified, Taronga will, as soon as practicable, take reasonable steps to notify affected individuals about the breach.

The CE will first consider if any exemptions apply to the notification of affected individuals, (see Section 5.9).

If no exemptions apply, affected individuals will be directly notified of the data breach by phone, email or letter.

Direct notification to affected individuals will, as far as reasonably practicable, include:

- Name of the agency (or agencies) the subject of the breach
- Contact details for Taronga or a person nominated as contact person for the breach
- Date of data breach
- Description of breach
- How the breach occurred
- Type of breach (eg unauthorised disclosure, unauthorised access, loss of information)
- Personal or health information that was the subject of the breach
- Amount of time of unauthorised disclosure / access
- Actions taken or planned to reduce harm resulting from the breach
- Recommendations for actions in response to breach
- Information about how to make a privacy related complaint or request an internal review (See Taronga's Privacy Management Plan)

5.8.1 Public notification of EDB

If it is not reasonably practicable to directly notify affected individuals, or Taronga is otherwise unable to notify affected individuals, a public notification register will be published on the Taronga website. The notification will be maintained for 12 months following the breach.

The notification register will provide available information regarding the data breach, including:

- Date of data breach
- Description of breach
- Type of data breach (eg unauthorised access, unauthorised disclosure, loss of information)
- Type of information subject to the breach
- Recommendations for actions in response to breach
- Date the public notification was published

5.9 Exceptions to the requirement to notify affected individuals

There are some circumstances where Taronga may be exempted from notifying affected individuals of an eligible data breach.

The use of any of the following exemptions must be fully documented and approved by the CE:

5.9.1 Multiple public sector agencies

Where a data breach involves multiple public sector agencies, and each agency has done an assessment and notified the Privacy Commissioner, one of the agencies may undertake to notify affected individuals. In this case, the other agencies are exempt from the requirement to notify affected individuals.

5.9.2 Ongoing investigations and proceedings

Taronga is exempt from the requirement to notify affected individuals if it is reasonably believed that notification of affected individuals is likely to prejudice an investigation that could lead to the prosecution of an offence, or prejudice proceedings before a court or tribunal.

5.9.3 Exemption based on mitigation action taken

Taronga is exempt from the requirement to notify affected individuals in cases where Taronga:

- Takes action to mitigate the harm done by the breach, and
- The action is taken before the breach results in serious harm to an individual, and
- Due to the action taken, it is not reasonably likely that the breach would result in serious harm to the individual

For example, the exemption may apply where the following occurs:

- A lost laptop containing personal information (and no security protection) is found before any unauthorised access
- Personal information mistakenly published on the internet is determined not to have been accessed, and is immediately taken down

5.9.4 Inconsistency with secrecy provisions

Taronga may be exempt from the notification requirements if compliance with the requirements would be inconsistent with a secrecy provision of legislation, that prohibits or regulates the disclosure of information.

5.9.5 Serious risk of harm to health or safety

The CE may decide to exempt Taronga from the requirement to notify affected individuals if they reasonably believe that notification would result in a serious risk of harm to a person's health or safety.

In making this decision, the CE must consider:

- The balance of whether the harm in notifying about the breach is greater than the harm in not notifying
- Any current information within the knowledge of the CE that goes to the question of risk of harm (but without accessing any data not affected by the breach)
- Guidelines issued by the Privacy Commissioner - Guidelines on the exemption for risk of serious harm to health or safety under section 59W, IPC, September 2023

If the CE seeks to rely on this exemption, Taronga will notify the Privacy Commissioner in writing that the exemption is being relied upon, the likely duration of the exemption and how the exemption will be reviewed.

The CE will provide an update to the Privacy Commissioner on each review of the exemption.

5.9.6 Cyber security

The CE may decide that an exemption applies from the requirement to notify affected individuals of an EDB, if it is reasonably believed that the notification would:

- Worsen Taronga's cyber security, or
- Lead to further data breaches

In making the decision to apply this exemption, the CE must consider the IPC Guideline - Guidelines on the exemption for compromised cyber security under section 59X, IPC, September 2023.

The exemption must only be in place for the period that Taronga's cyber security may be under threat, and the application of the exemption will be reviewed at least each month, to ensure that it is still necessary and applicable.

If the CE seeks to rely on this exemption, Taronga will notify the Privacy Commissioner in writing that the exemption is being relied upon, the likely duration of the exemption and how the exemption will be reviewed.

The CE will provide an update to the Privacy Commissioner on each review of the exemption.

5.10 Other notification requirements

5.10.1 Notification of TFN data breaches to Commonwealth OAIC

Taronga collects and stores the tax file numbers ('TFN') of staff and contractors to facilitate payments and wages.

The *Privacy Act 1988* (Cth) and the *Privacy (Tax File Number) Rule 2015* ('TFN Rule') apply to Taronga to mandate the notification of data breaches involving TFNs to the Office of the Australian Information Commissioner, ('OAIC').

Taronga will notify any breach involving TFNs to the OAIC (in addition to notifications under the PPIP Act) and comply with any additional notification requirements to affected persons in the TFN Rule.

Contact details for the OAIC:

Website: A report of a data breach involving TFNs may be made online through the OAIC website

Phone: The OAIC can be contacted on 1300 363 992

5.10.2 Notification to other bodies

Taronga will notify the Taronga Board and relevant external stakeholders of a data breach as required, including:

- Taronga's insurer, icare– Taronga must notify icare as soon as possible after becoming aware of an eligible data breach, significant data breach or cyber incident

- NSW Police, if criminal activity is suspected
- Cyber Security NSW or Cluster Chief Information Security Officers, as required under the NSW Cyber Security Policy
- NSW State Records – if the breach involves loss or damage of State archives
- Financial services providers, e.g. if bank accounts are suspected to be compromised
- Regulatory bodies or partner organisations / agencies
- Any third-party organisations or agencies whose data may be affected

5.11 Post-incident review

Taronga will carry out a post-incident review in relation to all data breaches involving Taronga's information that are assessed to be EDBs. The review will cover:

- Root cause analysis of the data breach and recommendations for prevention in future
- Review of Taronga's response and management of data breach including timeliness of initial internal reporting, efficacy of containment and mitigation measures, quality of assessment and efficiency and timeliness of notification to the NSW Privacy Commissioner and affected individuals
- Review of this Data Breach Policy and related plans in guiding management of the breach
- Review of related Taronga policies and procedures
- Identification of lessons learned and an action plan to implement any consequent improvements to systems or processes to address weaknesses.
- Actions taken to prevent future breaches

5.12 Record keeping requirements

Taronga must keep records of reports and action taken in relation to data breaches, in line with Taronga's Records Management Policy and *State Records Act 1998*.

In addition, Taronga keeps an internal register of all data breaches that have been determined to be EDBs.

The register is maintained by the Information Management Specialist and contains the following details:

- Type of breach
- Steps taken by Taronga to mitigate harm done by the breach
- Who was notified of the breach
- When the breach was notified
- Actions taken to prevent future breaches
- Estimated cost of the breach

6 Prevention and Preparedness

Taronga uses a number of systems and processes to strengthen and monitor cyber security, seeking to prevent data breaches from occurring and ensuring our preparedness in the event of a breach. Such processes include:

6.1 Implementing cyber security controls

Taronga implements IT systems and processes in line with the NSW Cyber Security Policy to ensure effective IT access controls, data security, integrity and availability.

6.2 Risk management

Taronga identifies, assesses, treats and monitors information management risk in operational and enterprise business processes in line with its Risk Management Policy and process.

Emerging risks are identified and risk treatments are reviewed regularly for effectiveness.

Data risk is reviewed and reported regularly to the Board / senior management in line with Taronga's Risk Management Policy and Procedure.

6.3 Training and awareness

Taronga provides training to ensure Taronga's people are aware of the risks and signs of data breaches, and the required response. Taronga's training program aims to prevent data breaches as far as possible and ensure Taronga is prepared to respond promptly and effectively, if they occur.

Taronga's training program covers:

- NSW privacy obligations relating to the collection, use, storage and disclosure of personal and health information
- Records management processes, including retention and disposal authorities
- Cyber security
- Guidance for Taronga's people on how to identify and report data breaches
- Guidance for CE, Executive and Assessors regarding data breach response process, assessment and how to manage reports.

Taronga's training program includes:

- Online training modules on topics such as cyber security, privacy, information management at Taronga's induction course and ongoing learning
- Regular staff forums and communication on privacy and cyber security topics, including information on current cyber risks and trends
- Educational fact sheets on cyber hygiene, identifying and reporting data breaches
- Easy report function for email phishing attempts and a 'friendly phishing' program
- Specialised training / awareness material for IT staff / response team relating to the management of eligible data breaches under this Policy, including considerations and escalation points in the assessment process

6.4 Testing of the Data Breach Policy

Taronga conducts regular testing of the Data Breach Policy and related plans to ensure that processes are current and effective. Lessons learnt in testing are incorporated into reviews of the Policy.

6.5 Clear provisions in third-party contracts

Taronga may engage contractors to carry out Taronga functions or provide services on behalf of Taronga. If so, Taronga ensures contractors comply with this Data Breach Policy and other information management policies, when carrying out Taronga functions.

Taronga ensures that third party service providers who use, store, manage or hold Taronga data are aware of the MNDB Scheme and their obligations under this Policy to report all real and suspected data breaches to Taronga.

7 Related Policies and Plans

The Data Breach Policy is to be read in conjunction with related Taronga policies, including:

- Risk Management Policy
- Privacy Management Plan
- Records Management Policy
- Cyber Security Policy
- Business Continuity Policy

8 Policy Review

This Data Breach Policy will be reviewed and updated annually or more frequently, if necessary following any changes, including regulatory change (eg the issue of updated IPC Guidelines), or changes in the nature or threat level of data breaches.

The review of the policy will take into account learnings from regular testing of the Data Breach Policy, the outcome of any post incident reviews of previous data breaches and an assessment of current trends and risks.

The Data Breach Policy is published on Taronga's website.

9 Responsibility and Accountability

All Taronga employees, volunteers, contractors, staff of contracted bodies engaged to perform Taronga functions	• Report all data breaches, suspected data breaches and possible data breaches to the IT Service Desk through Taronga's JIRA system immediately • Take all reasonable steps to contain a data breach and mitigate any harm likely to be caused by a breach • Be security aware - practice good cyber hygiene, report phishing attempts, password management; protect the physical security of information assets

	• Take part in induction and training exercises; provide informal training and awareness to team members about the importance of data security and reporting incidents • Support the assessment process and notification process of affected individuals in your business area • Participate in and / or assist the Data Breach Response Team through expert subject matter advice, if required • Include provisions in third party contracts to ensure compliance with this Policy
Chief Executive ('CE')	• Oversee Taronga's mandatory notification of data breach scheme • Direct a person or body to conduct an assessment of the data breach under s 59G PIPP Act • Make decisions to approve extension of time for s 59G assessment • Decide, on recommendation from the Assessor, whether a data breach is an eligible data breach • Make decisions regarding exemption from Taronga's notification requirements to affected individuals • Notify the Privacy Commissioner of an eligible data breach in the approved form, and update notification as required • Notify affected individuals directly or by public notification • Convene the Data Breach Response Team • Activate Taronga's business continuity / crisis management plan if required
Divisional Director, Corporate Services and Governance	• Convene and chair the Data Breach Response Team • Oversee initial assessment and triage of data breach • Direct a person or body to conduct an assessment of the data breach under s 59G PIPP Act • Approve an extension of time to conduct an assessment and notify Privacy Commissioner of extension • Decide, after receiving advice of Assessor, whether data breach is an eligible data breach • Notify the Privacy Commissioner of an eligible data breach in the approved form, and update notification as required • Approve and / or decide application of exemptions from the requirement to notify affected individuals • Notify affected individuals directly or by public notification
Divisional Director, People, Culture and Safety	• Convene the Data Breach Response Team • Oversee initial assessment and triage of data breach • Direct a person or body to conduct an assessment of the data breach under s 59G PIPP Act • Approve an extension of time to conduct an assessment and notify Privacy Commissioner of extension • Decide, after receiving advice of Assessor, whether data breach is an eligible data breach • Approve and / or decide application of exemptions from the requirement to notify affected individuals • Notify affected individuals directly or by public notification

	• Develop and maintain procedures for the reporting of TFN breaches • Design and deliver, in conjunction with IT, induction and ongoing training on cyber security, privacy and data breach reporting and management
Divisional Director, Marketing, Communications and Fundraising	• Convene the Data Breach Response Team • Oversee initial assessment and triage of data breach • Direct a person or body to conduct an assessment of the data breach under s 59G PIPP Act • Approve an extension of time to conduct an assessment and notify Privacy Commissioner of extension • Decide, after receiving advice of Assessor, whether data breach is an eligible data breach • Approve and / or decide application of exemptions from the requirement to notify affected individuals • Notify affected individuals directly or by public notification • Develop, maintain and implement communication plan for data breach notification and announcement to affected persons and stakeholders • Maintain crisis communication plans, templates and contact lists • Engage with media / the public in the event of a data breach requiring public notification
Director, Information Technology	• Oversee Taronga's information management program including knowledge management, classification and retention and disposal procedures • Oversee Taronga's cyber security program including implementation of Essential 8, IT access controls • Implement actions and advise on options to contain a data breach • Implement actions and advise on options for mitigating harm arising from a data breach • Assist in developing and delivering cyber security and data breach training to Taronga's people • Oversee data breach response under this Policy, including initial assessment and triage • Convene the Data Breach Response Team • Direct a person or body to conduct an assessment of the data breach under s 59G PIPP Act • Approve an extension of time to conduct an assessment and notify Privacy Commissioner of extension
Information Management Specialist, Information Technology	• Manage reports of data breach and conduct initial assessment • Implement and advise on actions to contain the data breach and mitigate harm resulting from the breach • Conduct initial assessment and triage of reports • Maintain Taronga's internal data breach register • Assist in assessment and response of data breaches
Assessors (persons or bodies directed to conduct assessment of	• Assess reports of possible eligible data breaches within 30 days, taking into account Statutory Guidelines – *Guidelines on the*

data breach under s 59G PPIP Act)	*assessment of data breaches under Part 6A of the PPIP Act, IPC September 2023* • Advise the CE if a data breach is an EDB, or if there are reasonable grounds to believe the data breach is an EDB.
Data Breach Response Team	• Decide on membership and nominate Chair (if Divisional Director Corporate Services and Governance is not available) • Direct, oversee and advise on immediate actions to contain the breach and mitigate any loss or harm caused by the breach • Assist decision makers in the assessment process by gathering information, providing subject matter expertise, providing recommendations and advice regarding actions including appointment of suitable Assessor • Advise on the application of exemptions from requirement to notify affected individuals • Coordinate and advise on notification actions under the Policy • Participate in post incident reviews
Privacy Officer / Manager Governance and Risk	• Manage reports of data breach • Develop, maintain, test, publish and review Taronga's Data Breach Policy • Develop, maintain and review Taronga's Privacy Management Plan • Design and establish Taronga's internal data breach register • Establish and maintain Taronga's public notification register • Support the actions of the Data Breach Response Team • Assist in development of education and awareness material, including flowcharts, checklists and fact sheets • Coordinate post-incident reviews of data breaches and implement improvement actions
Manager, Procurement, Contracts and Projects	• Advise on provisions in third party contracts to ensure compliance with this Policy

10 Version Control

Version Control	Date Effective	Drafted by	Approved By	Amendment
1.0	8 December 2023	Corporate Services and Governance	Board	New Policy as required by Pt 6A PPIP Act

11 Approval

Policy Owner	Governance and Risk / IT	**Divisional Director**	Corporate Services and Governance
Approval Authority	Board	**Approval Date**	8 December 2023

12 Appendix

Appendix A: Data Breach Assessment Process – Flow Chart