PORT AUTHORITY
OF NEW SOUTH WALES

PRIVACY MANAGEMENT PLAN

10 January 2022

Contents

CEO's Message

I am pleased to present the Port Authority of New South Wales Privacy Management Plan (Plan), developed in accordance with the requirements of section 33 of the Privacy and Personal Information Protection Act 1998 (NSW).

Port Authority is committed to providing services critical to the economy and infrastructure to the state of New South Wales whilst at the same time exhibiting social responsibility by having regard to the interests of the community in which it operates. This plan demonstrates a commitment by Port Authority to protect the privacy rights of our employees, stakeholders and members of the public in their interactions with Port Authority.

I urge all staff to read this Plan and use the procedures and message contained within to ensure Port Authority meets its privacy obligations.

Philip Holliday

Chief Executive Officer and Director

1 Introduction

Port Authority of New South Wales (Port Authority) takes the privacy of employees, stakeholders, customers and the public seriously and for this reason has chosen to voluntarily comply with the below mentioned Privacy Laws ahead of those laws coming into effect for state owned corporations in NSW.

1.1 Privacy Management Plan

This Privacy Management Plan (Plan) is an important tool in explaining how Port Authority upholds and respects the privacy of employees, contractors and others about whom it holds personal and health information, in accordance with the following key Privacy Laws:

- *Privacy and Personal Information Protection Act 1998 (*PPIPA*);* and
- *Health Records & Information Privacy Act 2002* (HRIPA).

The Plan is a requirement of section 33(2) of the PPIPA and explains:

- the policies and practices in place to achieve privacy compliance
- who to contact with questions about the information collected and held by Port Authority
- how to access and amend your personal information
- what to do if Port Authority may have breached its privacy obligations
- the internal review procedures in place.

Port Authority also applies the *Privacy Act 1998 (Cth)* in relation to personal information which is required to be handled in accordance with the federal privacy legislation e.g., Tax File Numbers of individuals.

The Privacy Management Plan covers all personal and health information, irrespective of whether it is collected from employees, customers, tenants, service providers, members of the public and/or other stakeholders.

This Plan is also used in training and as a reference for employees of Port Authority to understand and comply with their obligations. These obligations are reinforced by Port Authority's *Code of Conduct* and through initiatives outlined in this Plan (see 7.1 Roles and Responsibilities for more detail).

1.2 About us

Port Authority is a NSW State Owned Corporation responsible for managing the navigation, security and operational safety needs of commercial shipping in Sydney Harbour, Port Botany, Newcastle Harbour, Port Kembla, Eden and Yamba (ports).

Port Authority's statutory objectives and functions are derived from the provisions of the *State Owned Corporations Act 1989 (NSW), Ports and Maritime Administration Act 1995 (NSW)* and the *Port Safety Operating Licence* (PSOL) issued under section 12(2) of the *Ports and Maritime Administration Act*.

The principal functions of Port Authority include:

- to establish, manage and operate port facilities, cruise terminals, tenancies and services in its ports
- to exercise port safety and security functions which includes the installation and maintenance of navigation aids, vessel traffic control, pilotage services, providing emergency response and carrying out investigations into marine accidents or incidents
- to facilitate and co-ordinate improvements in the efficiency of the port-related supply chain and trade development including managing a towage licensing system.

This Plan will further explain how Port Authority collects and handles personal information for these purposes as well as how a person can exercise their rights in relation to their personal information.

1.3 Contact us

For further information about this Plan, any concerns about your privacy or questions about how Port Authority manages personal and health information please contact Port Authority's Privacy Coordinator as follows:

Post: GPO Box 25, Millers Point, SYDNEY NSW 2001
Email: access2info@portauthoritynsw.com.au
Website: www.portauthoritynsw.com.au
Phone: (02) 9296 4999

2 Personal and health information held by Port Authority

Port Authority collects, holds, uses and discloses personal information and health information for the purpose of carrying out its functions and general activities in running the business. This includes managing personnel files, procuring goods and services, securing sites and interacting with the community in relation to Port Authority's projects, proposals and activities.

2.1 What is Personal Information?

Personal information is defined in section 4 of the PPIPA as:

"…*information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion"*.

Essentially, personal information is any information or an opinion that can be used to identify an individual.

Information will only be considered persona if it is about an individual whose identity is "apparent or can reasonably be ascertained". For example, a person's identity may be ascertained without being named such as through a photograph or CCTV footage. Whether the identity of a person can reasonably be ascertained will depend on the type and combination of information and the context in which it is being used.

Common examples of personal information include an individual's name, contact details, identification, photograph, sound recording or video. A sample list of information that we may collect is set out in Annexure A for reference purposes.

2.1.1 What is not personal information?

There are certain types of information that are not considered personal information, and these are outlined at section 4(3) and section 4A of the PPIPA. Some of these include:

- information about an individual who has been dead for more than 30 years
- information about an individual that is contained in a publicly available publication (for example, information provided in a newspaper, social media, radio, television or court judgment available on the internet)
- information or an opinion about an individual's suitability for appointment or employment as a public sector official (for example, recruitment records, referee reports and performance appraisals).

2.2 What is Health Information?

Health information is a specific type of personal information that is defined in s6 of the HRIPA and includes information or an opinion about an individual's physical and mental health.

2.2.1 What is not health information?

As with personal information, there are certain types of information which are not considered 'health information'. These are outlined in section 5(3) of the HRIPA and include:

- health information of an employee who has been deceased for more than 30 years
- information regarding suitability for appointment or employment.

2.3 Employee Information

Annexure A lists examples of information that we collect or receive about employees and prospective candidates.

Personal information of employees is managed in accordance with this Plan. Where variations for employees exist (e.g., the in-house procedure for employees to access their personal or health information) the alternative will be detailed in the relevant section.

As stated above, information regarding a person's suitability for appointment or employment with Port Authority is not covered by the Privacy Laws, however the exemption does not apply to all employee information. Nevertheless, Port Authority will treat all employee related information with utmost care, whether or not an exemption applies.

2.4 Who do we collect from and who do we disclose to?

Port Authority may collect personal or health information from, or disclose personal or health information to, our stakeholders to do our work. Generally, these stakeholders include:

- employees, contractors and visitors
- tenants, operators and other persons conducting a business or undertaking
- insurers
- members of the public
- law enforcement agencies
- state and federal government agencies, regulators and authorities
- private sector companies
- State and Federal Ministers
- medical and allied health professionals
- solicitors and other legal representatives
- courts and tribunals.

3 Privacy Principles

The Privacy Laws set out 'privacy principles' that apply in handling personal and health information from the point of collection through to the point of disposal.

There are 12 Information Protection Principles (IPPs) set out in PPIPA for personal information and 15 Health Privacy Principles (HPPs) set out in HRIPA for health information.

The HPPs reflect the IPPs with some additional principles with respect to anonymity, the use of unique identifiers and the linking of electronic health records. These additional health protection principles are not relevant to Port Authority however should the activities of Port Authority change, the Plan will be reviewed.

The privacy principles set out the *minimum* standards for all NSW agencies handling personal and health information. Within these principles lawful exemptions are provided.

A list of the IPPs and HPPs can be found in Annexure B.

For ease of reference, the privacy principles are grouped into 4 main categories:

1. collection principles
2. use and disclosure principles
3. retention and security principles
4. sensitive information principles.

The next section details how Port Authority applies the IPPs and HPPs.

4 How Port Authority applies Personal and Health information protection principles

4.1 Collection of personal and health information

Key principles: *Collection of information must:*

- ✓ *be for a lawful purpose*
- ✓ *be collected directly from the individual*
- ✓ *meet specific notice requirements; and*
- ✓ *be relevant, not excessive, accurate and not intrusive.*

IPP & HPP 1-4

4.1.1 How we apply these principles

Lawful purpose

Port Authority will not ask for personal or health information unless it is directly related to our functions or activities, and its collection is reasonably necessary for us to perform those functions or activities. Port Authority will avoid or limit collecting sensitive personal information unless we need it to fulfil our functions, or it is necessary to a request, investigation, complaint or incident.

Relevant, not excessive, accurate and not intrusive

Port Authority will take reasonable steps to ensure that the personal and health information we collect is relevant, accurate, up-to-date, complete, is not misleading or unreasonably intrusive or excessive. For example, in certain functions we use standard forms or questionnaires so that no additional or unnecessary information is collected.

Direct from individual where possible

Port Authority will only collect personal and health information about a person from a third party where it is lawful to do so, or the individual has authorised collection of the information from someone else. Otherwise, collecting information direct from the source makes it easier for Port Authority to comply with other obligations too, like ensuring the accuracy of the information and getting permission for any secondary use or disclosure of the information.

Personal or health information may be collected in person, over the phone, by email, post, through use of Port Authority's website or applications (e.g., Port Management Systems), other affiliated websites, recruitment agencies, social media pages, or through participation at community events and visits to our offices and ports.

All employees, service providers, visitors, stakeholders, customers and other third parties should expect that their movements and activities are recorded via access card logs and CCTV when attending any Port Authority ports or sites they attend.

Notification

We will inform you at the time of collecting your personal information of the purpose for collecting it or otherwise as soon as practicable after the collection. This can be verbal, on display (e.g., where CCTV is being used) or in written form including via a 'privacy notice' in an application or form, our website or via a recorded message.

When interacting with Port Authority via telephone, radio or pilotage, individuals can expect that Port Authority will be recording the conversation in accordance with this Plan, PSOL and the *Surveillance Devices Act 2007 (NSW)* which includes seeking prior consent.

Consent to undertake audio recordings of private conversations and optical surveillance recordings could be obtained in various ways including as part of a contract with Port Authority (e.g., employment or service contract), site sign-in process, induction process, pre-recorded message, sign-off on a passage plan, signage on site with CCTV equipment or a verbal consent.

If an individual chooses not to provide certain personal or health information, Port Authority may not be able to action or respond to the request or permit certain activities.

4.2 Use and disclosure of personal and health information

4.2.1 How we apply these principles

Key Principles: *Port Authority must:*

- ✓ *check the information before using it to make sure it is relevant, accurate, and complete*
- ✓ *not use information for a purpose other than the collection purpose except in limited circumstances; and*
- ✓ *not disclose information for a purpose other than the collection purpose except in limited circumstances.*

IPP & HPP 9-11

Primary purposes

When Port Authority uses personal and health information, it means that we use it to fulfil a function of Port Authority. To fulfil these functions, we may need to provide personal information to service providers engaged to manage information on our behalf (e.g,. data hosting services).

Port Authority will only use personal and health information for:

- the primary purpose for which it was collected
- a purpose directly related to the primary purpose
- another purpose where it is reasonably necessary to prevent or lessen a serious and imminent threat to life or health of the individual to whom the information relates or of another person
- another purpose for which the individual has consented; or
- another purpose where required by law
- permissible secondary purposes.

Service providers who are contracted to assist us with our activities are required to only use personal information for the purposes of the contract and in accordance with the Privacy Laws or a privacy regime which has equivalent protections to the Privacy Laws. Service providers are not permitted to use personal and health information for a purpose other than the primary purpose for which it was collected by or on behalf of Port Authority.

Secondary purposes

Some examples of where the law permits Port Authority to use personal or health information for another (secondary) purpose include:

- quality assurance activities such as monitoring, evaluating and auditing
- use or disclosure under other legislation
- as permitted by law including work health and safety laws that requires Port Authority to use information to ensure the safety of our employees, port users and visitors; or
- unsatisfactory professional conduct, or breach of contractor policies.

Third parties

When Port Authority discloses information, it means that we give it to a third party outside Port Authority to use the information for their own purposes. We will only disclose personal or health information if:

- the disclosure is directly related to the purpose for which the information was collected
- the individual has consented and been made aware in the privacy notice that information of the kind in question is usually disclosed to the recipient
- we reasonably believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health; or
- the disclosure is otherwise authorised or required by law.

For example, under our PSOL, Port Authority must provide the Minister for Transport for NSW with certain information about its functions including but not limited to:

- a list of all persons holding valid Pilotage Exemption Certificates
- reporting on marine accidents/incidents involving a vessel that results in a serious injury or damage to property
- reporting on marine pollution incidents or accidents.

4.3 Retention and Security of personal and health information

***Key Principles**: Port Authority must:*

- ✓ *keep information only for as long as necessary for its lawful purposes for use*
- ✓ *dispose of information appropriately*
- ✓ *protect the information through appropriate safeguards against loss, unauthorised access, use, disclosure, misuse*
- ✓ *do everything reasonably required to protect information given to another person to provide a service to the authority.*

IPP & HPP 5

4.3.1 How Port Authority applies retention and security principles

Information security is fundamental to information privacy. As well as physical files, Port Authority uses a number of information systems to effectively handle and store personal and health information. To ensure information security and appropriate retention, Port Authority has a number of security measures in place including technical, physical and administrative processes to safeguard information from unauthorised access, loss or other misuse, including:

- restricting access to all IT systems and databases to ensure that only authorised users with a clear business need can access them. Adopting the principle of 'least privilege' and 'segregation of privilege' users of critical systems operate using the minimum level of privileges necessary to complete their work.
- requiring use of strong passwords for access to computers, networks, platforms and applications, with a mandatory requirement that all employees change access passwords on a regular basis.
- implementing and maintaining security software across all network components backup and storage (including encryption, multi-factor authentication and password protection where appropriate).
- providing employees with access to secure physical storage spaces to secure documents and devices.
- Monitoring, recording and auditing access to systems.
- maintaining and continually improving information security management systems.
- auditing the information security framework and conducting adequacy assessments on a regular basis by internal and independent parties.
- adopting best practice in electronic and paper records management and complying with the obligations under the *State Records Act 1998 (NSW)* including the adoption of Port Authority Records Destruction Policy and Procedure and Normal Administrative Practice Policy.
- Segregating operational networks and systems behind firewalls.
- where it is necessary for information to be held by a third party provider to provide us with a service (e.g. hosting), conducting a risk assessments and executing contract terms to govern third parties'

access and use of personal and health information consistently with the Privacy Laws and prevent unauthorised use or disclosure.
- undertaking periodic employee awareness initiatives and induction training.
- ensuring employees and contractors can only access physical sites using secure card access according to their security clearances.

Related Policies:
- *Port Authority Records Destruction Policy and Procedures*
- *Normal Administrative Practice Policy*
- *IT Security Policy*
- *IT Password Policy*
- *IT Security Incident Management Procedure v2.0*
- *Fraud and Corruption Policy*

4.4 Special restrictions

Key Principles: *Port Authority must adhere to special requirements when disclosing or transferring:*
- ✓ *"sensitive information"*
- ✓ *personal and health information outside of NSW; and*
- ✓ *Tax File Numbers.*

IPP 12 (sections 18, 19), HPP 14, TFN Rule

4.4.1 How we apply these principles

Sensitive Personal Information

Port Authority recognises that additional protection should be given to "sensitive personal information" which include an individual's:
- ethnic or racial origin
- political opinions
- religious or philosophical beliefs
- trade union membership.

Port Authority may only disclose sensitive personal information when the individual has consented to the disclosure or when it is necessary to prevent a serious and imminent threat to life or health, or to comply with legislation.

Transborder Transfers

Transfer of any personal information or health information outside of NSW or to a Commonwealth Agency is only permitted in strict circumstances, including where:
- the disclosure is required to comply with legislation or statutory reporting requirements
- the disclosure is necessary to prevent or lessen a serious and imminent threat to life, health or safety
- the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the IPPs or HPPs
- Port Authority has taken reasonable steps to ensure that the information will be handled consistently with the Privacy Laws and only for the purpose for which it was disclosed; or
- the individual has consented to the disclosure.

In cases where Port Authority must use or refer to personal or health information, we will consider anonymising the data first where possible, particularly if an individual's details are not required (for instance summary data of health incidents).

Tax File Numbers (TFN)

Port Authority, as a TFN recipient employer, must only record, collect, use or disclose TFN information where permitted under taxation, personal assistance or superannuation law. Individuals are informed of the purpose of collection and that they have a right to decline quoting a TFN as long as the consequences of not providing a TFN are made known to the individual.

Port Authority can only use or disclose TFN information for a purpose authorised by taxation law, personal assistance law or superannuation law, or where the individual has requested TFN information held by Port Authority.

4.5 Exemptions from the Privacy Principles

There are exemptions to the application of the IPPs and HPPs which means that Port Authority can collect, use and disclose information in limited situations without following the privacy principles.

For example, the IPPs and HPPs do not apply:

- where a law lawfully permits non-compliance (for e.g., expressly permits disclosure of information which otherwise could not be disclosed) (s 25 PPIPA)
- if the information concerned is collected in relation to court or tribunal proceedings (s23 PPIPA)
- in the event of a serious and imminent threat to the life, health and safety of an individual (s19(f) PPIPA; Schedule 1, cl10(1)(c) and 11(1)(c) HRIPA)
- if the information is required to be used for law enforcement purposes, investigations or the protection of public revenue (s23, 24 PPIPA; Schedule 1, cl 10(1)(g) –(j) and 11(1)(i) –(k) HRIPA).

5 How to access and revise personal / health information

5.1 Individuals accessing and revising their personal information

Key Principles: *Port Authority must:*

- ✓ *take reasonable steps to enable any person to ascertain details of the information the authority holds about them and the purpose it was collected*
- ✓ *when requested provide individuals with access to their information without excessive delay or expense; and*
- ✓ *make appropriate amendments or make notations to ensure the information remains accurate, relevant, up-to-date, complete and not misleading.*

IPP & HPPs 6-8

Port Authority encourages individuals to keep personal and/or health information up-to-date and accurate, particularly information about personal contact details and next of kin contact details in case of an emergency.

Port Authority is required to provide an individual with access to their personal and/or health information we hold and allow them to amend this information to correct inaccuracies without excessive delay or expense unless an exemption applies. Please note that information is retained according to Port Authority's Records Destruction Policy and Procedure and Normal Administrative Practice Policy. As such, access is provided to those records available at the time of a request.

A formal application to access personal or health information held by Port Authority can be made by completing the Access Request and sending to:

Attention:	Privacy Coordinator
Post:	GPO Box 25, Millers Point, SYDNEY, NSW 2001
Email:	access2info@portauthoritynsw.com.au
Phone:	(02) 9296 4999

The Access Request form is shown in Annexure C. Alternatively, an informal application can also be made by sending an email to the Privacy Coordinator (or if you are an employee, you can send your request to People & Culture).

There is no fee to access or amend personal information under the PPIPA however a fee is payable to access or amend health information unless you are an employee of Port Authority (refer to Access Request form for fee and payment details).

5.2 Employees accessing and revising their personal and health information

Consistent with Port Authority's procedures under the *Government Information (Public Access) Act 2009 (NSW)* (GIPAA), employees can access their personnel files and any personal or health information held by Port Authority by making a request in writing to the Head of People & Culture.

5.3 Accessing or amending other people's information

Privacy Laws give people the right to access their own information, but they do not give people the right to access someone else's information, unless that individual has given consent in writing for an "authorised representative" (s 9 PPIPA) to act on their behalf.

The Privacy Laws permit Port Authority to disclose health information to a third party in very limited circumstances, such as in the event of a serious and imminent threat to the life, health and safety of the individual or another person, in order to help find a missing person, or for compassionate reasons (s11 HRIPA).

If none of these circumstances are relevant, a third party can consider making an application for access to information under GIPAA however there are similar restrictions to releasing personal and health information which may be applicable. For more information or to make an access application under GIPAA, please visit the Access to Information page of Port Authority's website.

6 Misuse of Information

The PPIPA and HRIPA contain criminal offence provisions applicable to public sector officials and persons (including current and former employees) who misuse personal and health information.

For example, it is a criminal offence to:

- intentionally disclose or use personal or health information for an unauthorised purpose
- offer to supply personal or health information that has been disclosed unlawfully
- attempt to dissuade a person from making or pursuing a request for health information, a complaint to the Privacy Commissioner or an internal review under the HRIPA
- cause any unauthorised access to or modification of restricted data held in a computer.

(s.62 of the PPIPA, s.68 of the HRIPA, and s.308H of the Crimes Act 1900)

Accordingly, this Plan is intended to assist employees to understand and comply with their obligations under the Privacy Laws.

If an employee is uncertain about their privacy obligations, they should seek the advice of the Privacy Coordinator.

Employees who are suspected of conduct which would breach the privacy principles or the criminal provisions will be referred to People & Culture for review.

7 Port Authority's strategies for compliance

Port Authority recognises that privacy is a shared responsibility within the organisation and accordingly has adopted several strategies to implement best practice principles and comply with our obligations.

The Executive team is committed to the transparency and accountability in respect of Port Authority's compliance with the Privacy Laws.

7.1 Roles and Responsibilities

7.1.1 Chief Executive Officer

The Chief Executive Officer, as Senior Responsible Officer, is responsible for compliance with the requirements of the Privacy Laws.

7.1.2 Group Executive

The Group Executive are responsible for supporting and considering compliance with this Plan and related procedures when implementing new projects, approving initiatives and in usual operations.

7.1.3 Privacy Coordinator (Corporate Services)

The Privacy Coordinator is responsible for managing the privacy framework across Port Authority including advising, assisting and supporting employees in complying with this Plan and its associated procedures as well as attending to Access and Internal Review requests. The Privacy Coordinator will assist the business in conducting privacy impact assessments for new initiatives (technology, procurement of services) or change in processes which have an effect on the handling of personal information.

7.1.4 Managers

Managers across the organisation (including Group Executive) are responsible for ensuring that privacy compliance is integrated into standard work processes, systems and services. Managers are responsible for their division's compliance with the Plan and procedures and will assist the Privacy Coordinator (Corporate Services) with monitoring and employee breaches of this Plan. Managers are responsible for overseeing compliance of service providers and making appropriate arrangements with service providers to ensure that they comply with the Plan.

7.1.5 Employees

All employees (including contracted employees and consultants) are responsible for handling personal and any health information in accordance with this Plan. Employees are required to familiarise themselves with their privacy obligations and responsibilities including attending privacy, record management and IT security training and escalating suspected data breaches to the Data Breach Response Team.

7.1.6 Information Technology

Information Technology is responsible for ensuring that privacy compliance is assessed and addressed in the scope of all new systems and service arrangements; following the advice and instructions of Privacy Coordinator; conducting cyber security training; investigating technical data breaches and ensuring that regular tests, audits and integrity checks of the operating environment are undertaken.

7.2 Policies and Procedures

Port Authority is committed to

- the requirement to comply with privacy legislation when handling personal and health information
- conducting reviews of systems and practices to inform changes required to ensure and maintain compliance
- monitoring changes in the legislative, policy or operational environment for their impacts on Port Authority's privacy management
- conducting privacy impact assessments to assess new projects and changes to policies and systems.

This commitment includes the formation of this Privacy Management Plan, and the following applicable policies which aid Port Authority in addressing the principles:

- Acceptable Use Policy
- Access to Information Policy
- Code of Conduct
- IT Vendor Security Guidance
- IT Acceptable Use Policy
- IT Password Policy
- IT Security Policy
- Normal Administrative Practice Policy
- Records Destruction Policy and Procedures
- Records Management Policy
- Procedures in Handling a Data Breach
- Fraud and Corruption Policy

7.3 Promoting privacy awareness

Port Authority will be undertaking a range of initiatives to ensure our employees, service providers, members of the public and other stakeholders are informed of our privacy practices and obligations under the Privacy Laws.

Port Authority promotes privacy awareness and compliance by:

- Executives endorsing a culture of good privacy practice including the endorsement of this Plan and initiatives for raising awareness and best practices
- publishing and promoting this Plan and Privacy Statement on both the intranet and public website
- using the plan as part of induction for new employees and service providers
- conducting training and awareness initiatives for all employees
- organisational risk review and audits to include privacy and information security considerations
- providing information and support to employees dealing with privacy matters
- assessing privacy impacts of new projects or processes from the earliest opportunity by conducting a Privacy Impact Assessment
- incorporating privacy management requirements into contracts with service providers
- promoting the plan at least once a year to all stakeholders (including during Privacy Awareness Week).

Privacy compliance has been designed to fit within the framework of Port Authority's obligations, practices and priorities in mind to ensure that privacy considerations become part of the way we do business.

Port Authority is subject to other legislation which may impact the way it handles personal and health information. Examples of legislation as at the date of this Plan include:

- Public Health (COVID-19 Maritime Quarantine) Order (No 4) 2020 under the Public Health Act 2010
- Biosecurity Act 2015 (Cth)
- Environmental Planning and Assessment Act 1979 (NSW)
- Marine Safety Act 1998 (NSW)
- Marine Pollution Act 2012 (NSW)
- Maritime Transport and Offshore Facilities Security Act 2003 (Cth)

- Ports Assets (Authorised Transactions) Act 2012 (NSW)
- Protection of the Environment Administration Act 1991 (NSW)
- Work Health and Safety Act 2011 (NSW)
- Government Information (Public Access) Act 2009
- State Records Act 1998
- Surveillance Devices Act 2007 (NSW)
- Workplace Surveillance Act 2005.

7.4 Review, learn and improve

Port Authority will evaluate the effectiveness and appropriateness of its privacy practices, policies and procedures to ensure they remain effective and to identify, evaluate and mitigate risks of potential non-compliance.

Port Authority is committed to:

- monitoring and reviewing its privacy processes
- further promoting and maintaining privacy awareness and compliance.
- encouraging feedback from staff on our privacy practices
- introducing initiatives that promote good privacy handling in our business practices (such as assessing privacy impacts of new projects or processes from the outset)
- carrying out regular audits / risk assessments on our digital information and technology systems
- promoting information security awareness to employees, to ensure information security compliance is fundamental in day-to-day activities
- making this Plan publicly available as open access information under GIPAA.

8 Your rights

8.1 Requesting an internal review

Any person can make a complaint and apply for a formal internal review of the conduct they believe breaches the law, IPP or HPP.

An internal review is a formal process by which Port Authority investigates privacy concerns about Port Authority's handling of personal information or health information.

All written correspondence about privacy is considered to be an application for internal review, even if the applicant doesn't use the words 'internal review'. If an individual would prefer to resolve their privacy concern informally, this should be noted when they contact Port Authority (see 8.1.4).

8.1.1 Lodging an application for an internal review

An application for internal review should:

- be in writing
- be addressed to Port Authority
- specify an address in Australia at which the person can be notified after the completion of the review.
- Detail the behaviour or information of concern which the applicant would like reviewed.

To apply for an internal review, complete the Application Form – Internal Review (attached as Annexure D) and send the application and any relevant material by email or post to:

Attention:	Privacy Coordinator
Post:	GPO Box 25, Millers Point, SYDNEY NSW 2001
Email:	access2info@portauthoritynsw.com.au
Phone:	(02) 9296 4999

8.1.2 Internal Review process

The internal review will be conducted by a person who:

- was not involved in the conduct which is the subject of the complaint or review
- is an employee of Port Authority; and
- is qualified to deal with the subject matter of the review and is endorsed by the relevant Executive.

When the internal review is completed, the applicant will be notified in writing of:

- the findings of the review
- the reasons for those findings
- the action Port Authority proposes to take
- the reasons for the proposed action; and
- the applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal (NCAT).

Port Authority will keep the Privacy Commissioner informed of the progress of the internal review and will supply a copy of your internal review request as well as the draft and final internal review report to the Privacy Commissioner.

8.1.3 Timeframes for Internal Reviews

You must lodge your request for internal review within six (6) months from the time you first became aware of the conduct that you think breached your privacy. A late application may be accepted in certain circumstance. If a late application is not accepted, then you will be provided with a written explanation.

Port Authority will formally acknowledge receipt of an application for internal review and will aim to:

- complete the internal review within 60 calendar days and
- respond in writing within 14 calendar days of completing the internal review (section 53 (8) of the PPIPA).

Should an internal review be likely to take longer than the prescribed 60 days, Port Authority will contact the applicant to advise a revised timeframe and the reason for the delay (as appropriate) and propose an extension of the review period. The applicant is not obliged to agree to an extension.

If the internal review is not completed within the timeframes specified or agreed, the applicant has the right to seek a review of the conduct by NCAT.

Please note that information is retained by Port Authority for prescribed times according to Port Authority's approved retention periods under the State Records Act and related Port Authority policies. For example, audio, CCTV and voice recordings are generally kept for 28 days only.

Consequently, if a person has a concern about the handling of such information or would like to request access to the information containing their personal or health information, Port Authority encourages them to contact Port Authority as soon as possible before the information is routinely destroyed/overwritten as we may not be able to retrieve those records after the prescribed time of retention.

8.1.4 Other ways to resolve privacy concerns

Port Authority welcomes the opportunity to discuss any privacy issues you may have. You are encouraged to try to resolve privacy issues with us informally before lodging an internal review.

You can raise your concerns with Port Authority by contacting access2info@portauthoritynsw.com.au.

Please keep in mind that you have six (6) months from when you first became aware of the potential breach to seek an internal review. This six (6) month time frame continues to apply even if attempts are being made to resolve privacy concerns informally. Please consider this time frame when deciding whether to make a formal request for internal review or continue with informal resolution.

8.2 Requesting an external review

If a person is unhappy with the outcome of an internal review conducted by Port Authority or do not receive an outcome within 60 days (or the agreed period), they have the right to seek an external review by NCAT.

A person has 28 calendar days from the date of the internal review decision to seek an external review under s53 of the *Administrative Decisions Review Act 1997 (NSW).*

To request an external review, you must apply directly to NCAT, which has the power to make binding decisions on an external review.

To apply for an external review or to obtain more information about seeking an external review, including current forms and fees, please contact NCAT. NCAT's contact details are:

Office:	NSW Civil and Administrative Tribunal Level 9, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000
Post:	PO Box K1026, Haymarket NSW 1240
Website:	http://www.ncat.nsw.gov.au
Phone:	1300 006 228

NCAT cannot give legal advice, however the NCAT website has general information about the process it follows and legal representation options.

8.3 Complaints to the Privacy Commissioner

Individuals have the option of complaining directly to the Privacy Commissioner if they believe that Port Authority has breached their privacy.

The Privacy Commissioner's contact details are:

Office:	NSW Information & Privacy Commission Level 17, 201 Elizabeth Street Sydney NSW 2000
Post:	GPO Box 7011 Sydney NSW 2001
Website:	https://www.ipc.nsw.gov.au
Phone:	1800 472 679
Email:	ipcinfo@ipc.nsw.gov.au

If the data concerned is governed by the *Privacy Act 1988 (Cth)* such as TFNs, individuals have the option to go directly to the the Commonwealth Privacy Commissioner at the Office of the Australian Information Commissioner (OAIC) by completing the form.

The OAIC's contact details are:

Office:	Office of the Australian Information Commissioner 175 Pitt Street Sydney NSW 2000
Post:	GPO Box 5218, Sydney NSW 2001
Website:	https://www.oaic.gov.au
Phone:	1300 363 992
Email:	enquiries@oaic.gov.au

9 Data Breach Management

We are committed to protecting personal information however there may be situations where data or systems are accessed or used contrary to the Privacy Laws. Port Authority continually monitors its systems, processes and practices and investigates data breaches or suspected data breaches as part of its commitment to the handling and security of personal information and health information.

Port Authority has a procedure in place for handling data privacy breaches which takes into account the guidelines of the NSW Information Privacy Commissioner.

Notifiable Data Breach Scheme

In relation to data which is governed by the Commonwealth regime (Privacy Act 1988 (Cth)) e.g., TFNs, Port Authority will assess the breach against each of the following criteria:

- the breach is likely to result in serious harm or impact to any of the individuals to whom the information relates; and
- Port Authority has been unable to prevent the likely risk of serious harm with remedial action. In other words, the risk of serious harm is more probable than possible to occur.

“Serious harm” for the purposes of assessing a data breach is taken to include such things as serious financial, physical, psychological, emotional or reputational damage, injury or impairment.

If the above criteria are met, Port Authority will notify the Commonwealth Privacy Commissioner OAIC under the Notifiable Data Breach Scheme.

Annexure A – Examples of Personal and Health information held by Port Authority

Below are common examples of personal and health information collected and retained by Port Authority in the exercise of its functions. Depending on the circumstances or the request by the individual, we may collect other personal and health information necessary for the situation and for different purposes as disclosed. In other words, the list below is not exhaustive and there may be other stated purposes, and there may be occasions where individuals disclose more information than what we request.

<table>
<tr><th colspan="2">Personal information collected by Port Authority about employees and service providers may include:</th></tr>
<tr>
<td>Purpose of collection may include:
assessment and management of recruitment and employment,
assessing tenders or requests for contractors,
discharge of statutory obligations and PSOL.
Facilitating coaching and training.
Conducting investigations (such as suspected or actual accident, incident, breach of contract or policy, allegation, grievance, claim or complaint).</td>
<td>Personal information:
Personnel files
Information held on the People and Culture information database (e.g., address, salary details, birth date)
Payroll information (e.g., salary details, bank account details)
Disciplinary files
Leave applications
Investigation files (safety, grievance, details of conduct)
Accident/incident records
Records of interview
Performance management and feedback records
Competency assessments, Certificate of Local Knowledge, MCIS details and training records and supporting documentation
Job applications, third party assessments (recruitment tools such as psychometric tests) and regulatory checks (e.g., police checks).
Images of individuals recorded on Port Authority’s CCTV surveillance system
Information required to comply with PSOL
Health information:
Sick leave information such as leave applications, medical certificates
Workers compensation files and claim forms
Urine drug analysis test results
Saliva drug analysis test results
Alcohol breath test results
Medical reports including fitness for duty assessments.</td>
</tr>
</table>

Personal information collected by Port Authority about third parties:	
Purpose of collection may include: • responding to a request, • processing payments, • investigating a complaint or incident, • assessing information on a project, • maintaining security of Port Authority assets, • discharging Port Authority functions and PSOL.	Personal Information: • Contact details (name, number) of visitors to Port Authority • Information provided as part of a request for information on our website • Information collected in answering a query or complaint on our website, email or telephone • Credit card details for purchases • Accident/Incident information • Details from members of the public during a local meeting including opinions • Personal identifying information for the purposes of accessing Port Authority systems • CCTV footage or voice/radio recording of VTS/VTIS communications or recordings of calls made to customer service hotline Health Information: Health Information collected by Port Authority about members of the public may include but may not be limited to: • medical information relating to personal injury claims for insurance claims • details required for Port Authority certifications and permits to assess Port Authority sites • health declarations required to access Port Authority sites.
For the Ports of Newcastle, Sydney Harbour, Botany Bay and Port Kembla	
Purpose of collection may include: • complying with statutory obligations and PSOL	Personal and/or Health Information: As required by the PSOL, recording capability enable all communications made with vessels to be recorded 24 hours a day, seven days a week throughout the year.

Annexure B – Privacy Principles

Part 1: Information Privacy Principles

Part 2, Division 1 of the PPIPA contains 12 IPPs with which Port Authority must comply:

Collection

1. Port Authority collects personal information only for a lawful purpose that is directly related to Port Authority's functions and activities.
2. Port Authority collects personal information directly from the person concerned unless they have authorised collection from someone else, or if the person is under the age of 16 and the information has been provided by a parent or guardian.
3. Port Authority informs people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. Port Authority will tell people how they can access and amend their personal information and any possible consequences if they decide not to give their personal information.
4. Port Authority ensures personal information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of individuals.

Storage

5. Port Authority stores personal information securely, keeps it no longer than necessary and destroys it appropriately. Personal information is protected from unauthorised access, use, or disclosure.

Access and accuracy

6. Port Authority is transparent about any personal information that is stored, what it is used for and the right to access and amend it.
7. Port Authority allows individuals to access their own personal information without unreasonable delay or expense.
8. Port Authority allows individuals to update, correct, or amend their personal information where necessary.
9. Port Authority makes sure that personal information is relevant and accurate before using it.

Use

10. Port Authority only uses personal information for the purpose it was collected for unless the individual has given their consent or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person's health or safety.

Disclosure

11. Port Authority will only disclose personal information with an individual's consent unless they were already informed of the disclosure when the personal information was collected; or if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object; or the person has been made aware that information of that kind is usually disclosed;or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.
12. Port Authority does not disclose, without consent, sensitive personal information such as ethnicity or racial origin, political opinions, religious or philosophical beliefs, sexual activities, or trade union membership unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person.

Part 2: Health Privacy Principles (HPP)

Schedule 1 of the HRIPA contains 15 HPPs with which Port Authority must comply. Below is an overview of the principles, as they apply to Port Authority.

Collection

1. Port Authority collects health information only for lawful purposes that are directly related to Port Authority's functions and activities.
2. Port Authority makes sure health information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.
3. Port Authority collects health information directly from the person concerned.
4. Port Authority informs people why their health information is being collected, what it will be used for and to whom it will be disclosed. Port Authority will tell people how they can access and amend their health information and any possible consequences if they decide to not give their health information to Port Authority.

Storage

5. Port Authority stores health information securely, keeps it no longer than necessary and destroys it appropriately. Health information is protected from unauthorised access, use, or disclosure.
6. Port Authority is transparent about the health information stored about people, what the information is used for and the right to access and amend it.
7. Port Authority allows people to access their own health information without unreasonable delay or expense.
8. Port Authority allows people to update, correct, or amend their health information where necessary.
9. Port Authority makes sure the health information is relevant and accurate before using it.

Use

10. Port Authority only uses health information for the purpose for which it was collected, unless the person consents to the information being used for an unrelated purpose.

Disclosure

11. Port Authority will only disclose health information with people's consent, unless they were already informed of the disclosure when the health information was collected.

Identifiers and anonymity

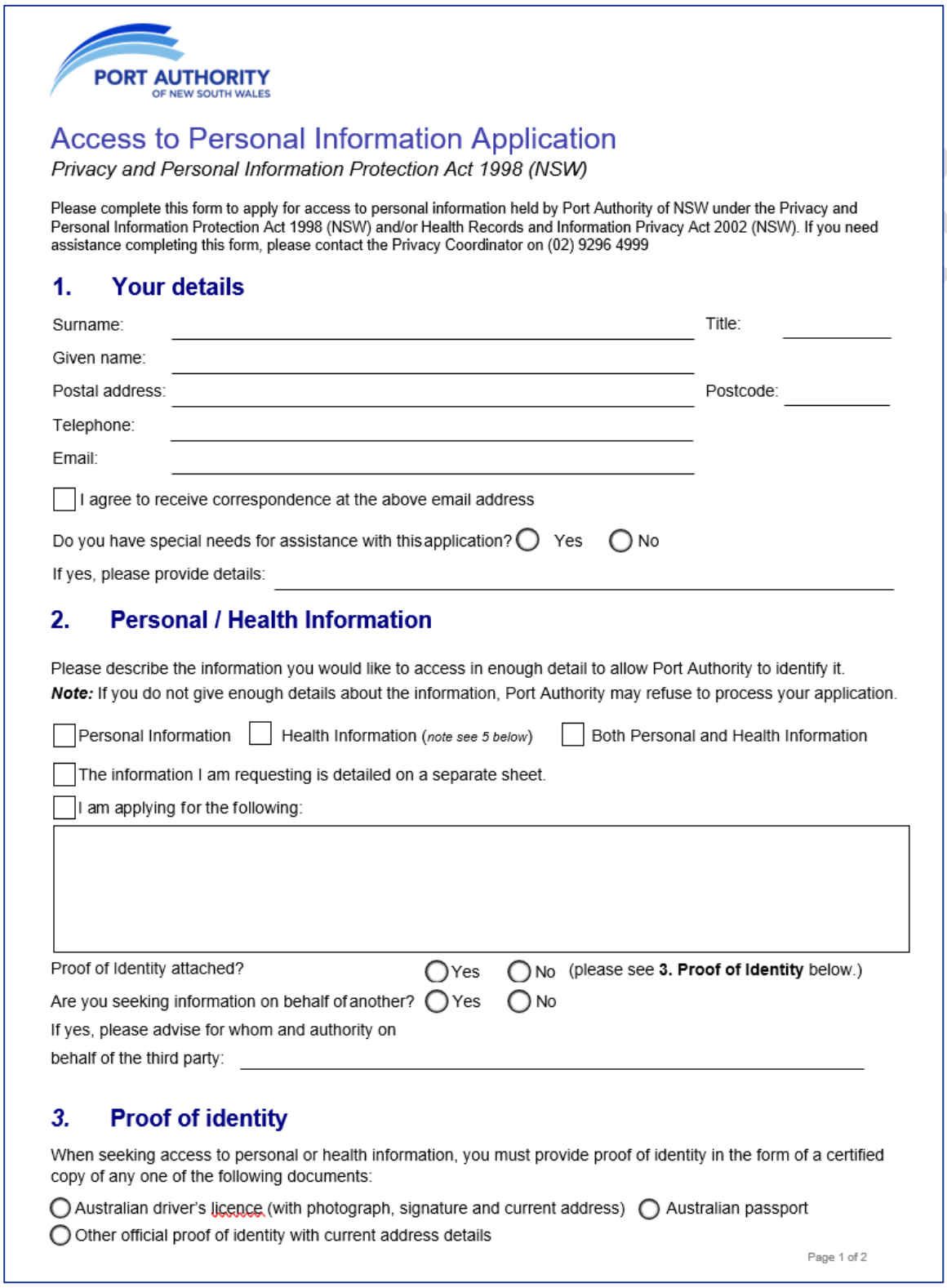
12. Port Authority does not use unique identifiers for health information, as they are not needed to carry out the functions of Port Authority.
13. Port Authority allows people and their health information to stay anonymous where it is lawful and practical.

Transfers and linkage

14. Port Authority only transfers health information outside of NSW where an exemption applies.
15. Port Authority does not currently use a health records linkage system and does not anticipate using one in the future.

Annexure C - Application Form: Privacy Request

The electronic version of this application form can be accessed here.



PORT AUTHORITY
OF NEW SOUTH WALES

Access to Personal Information Application

Privacy and Personal Information Protection Act 1998 (NSW)

Please complete this form to apply for access to personal information held by Port Authority of NSW under the Privacy and Personal Information Protection Act 1998 (NSW) and/or Health Records and Information Privacy Act 2002 (NSW). If you need assistance completing this form, please contact the Privacy Coordinator on (02) 9296 4999

1. Your details

Surname: _____ Title: _____

Given name: _____

Postal address: _____ Postcode: _____

Telephone: _____

Email: _____

☐ I agree to receive correspondence at the above email address

Do you have special needs for assistance with this application? ◯ Yes ◯ No

If yes, please provide details: _____

2. Personal / Health Information

Please describe the information you would like to access in enough detail to allow Port Authority to identify it.
Note: If you do not give enough details about the information, Port Authority may refuse to process your application.

☐ Personal Information ☐ Health Information (*note see 5 below*) ☐ Both Personal and Health Information

☐ The information I am requesting is detailed on a separate sheet.

☐ I am applying for the following:

Proof of Identity attached? ◯ Yes ◯ No (please see **3. Proof of Identity** below.)

Are you seeking information on behalf of another? ◯ Yes ◯ No

If yes, please advise for whom and authority on behalf of the third party: _____

3. Proof of identity

When seeking access to personal or health information, you must provide proof of identity in the form of a certified copy of any one of the following documents:

◯ Australian driver's licence (with photograph, signature and current address) ◯ Australian passport

◯ Other official proof of identity with current address details

Page 1 of 2

4. Form of access

How do you wish to access the information?

- ○ Inspect the document(s)
- ○ A copy of the document(s)
- ○ Access in another way (please specify) _____

5. Application Fee – Health Records Information Request

Under the Privacy and Personal Information Protection Act 1998 (NSW) and/or Health Records and Information Privacy Act 2002 (NSW), Port Authority may charge a fee for (i) giving an individual a copy of health information, (ii) giving an individual an opportunity to inspect and take notes of the health information, or (ii) amending health information.

If you have made a request for health information, an application is not valid without the payment of an application fee. Please select the option you have chosen to pay the fee:

- ○ I have made an electronic funds transfer to Port Authority of NSW: BSB 062-000 Account Number 1041 7500 (Please include "HRIP Request" in the reference)
- ○ I attach payment of the $30 application fee by cheque / money order. (please make payable to "Port Authority of New South Wales")

Applicant's lodgment

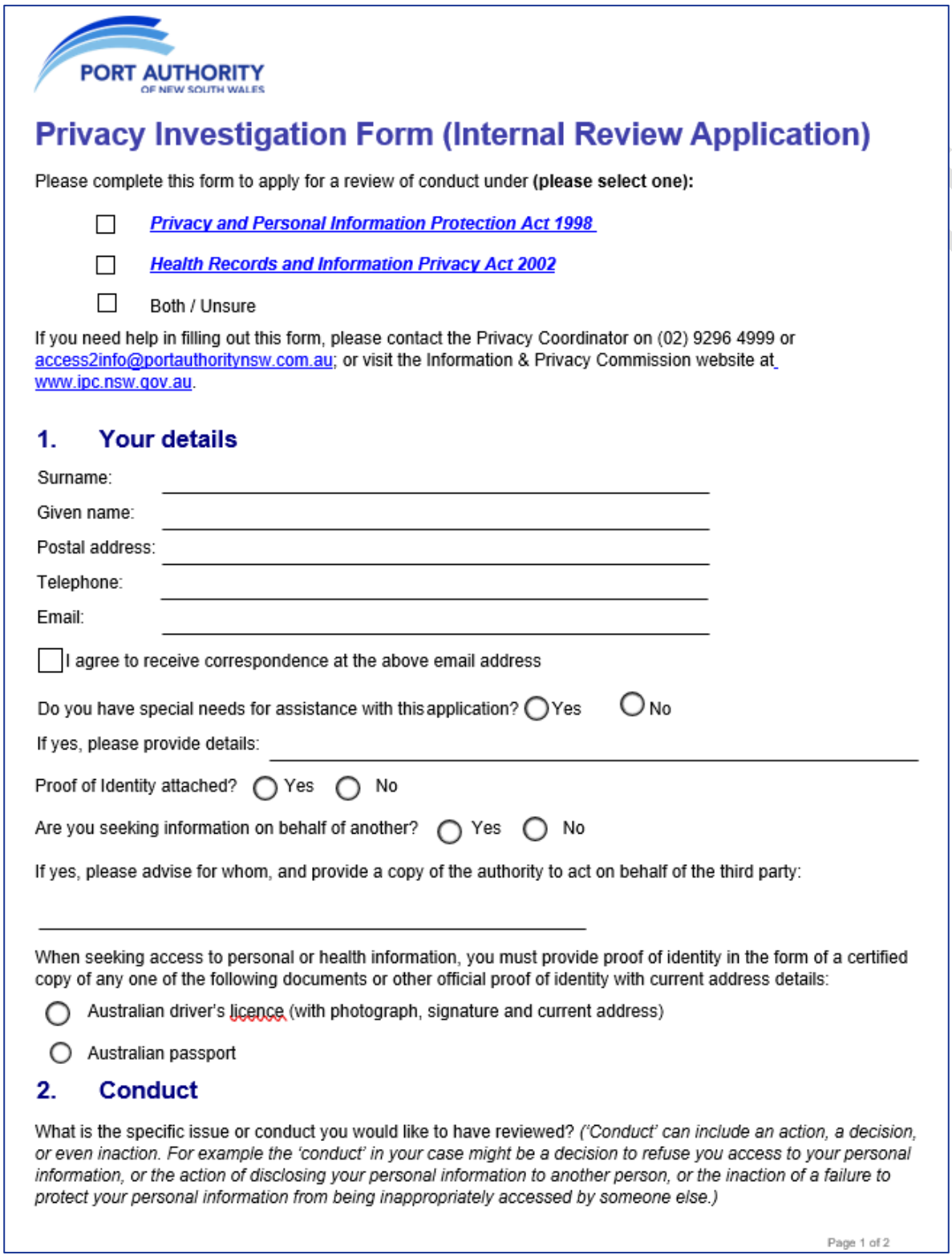
I understand that the information in this form will be used by Port Authority to process my request.

Please post/email this form with the application fee to:

Attention: Privacy Coordinator
Post: GPO Box 25, Millers Point, SYDNEY NSW 2001
Email: access2info@portauthoritynsw.com.au

Annexure D - Application Form: Internal Review

The electronic version of this application form can be accessed here.



PORT AUTHORITY
OF NEW SOUTH WALES

Privacy Investigation Form (Internal Review Application)

Please complete this form to apply for a review of conduct under **(please select one):**

- ☐ ***Privacy and Personal Information Protection Act 1998***
- ☐ ***Health Records and Information Privacy Act 2002***
- ☐ Both / Unsure

If you need help in filling out this form, please contact the Privacy Coordinator on (02) 9296 4999 or access2info@portauthoritynsw.com.au; or visit the Information & Privacy Commission website at www.ipc.nsw.gov.au.

1. Your details

Surname: _____

Given name: _____

Postal address: _____

Telephone: _____

Email: _____

☐ I agree to receive correspondence at the above email address

Do you have special needs for assistance with this application? ◯ Yes ◯ No

If yes, please provide details: _____

Proof of Identity attached? ◯ Yes ◯ No

Are you seeking information on behalf of another? ◯ Yes ◯ No

If yes, please advise for whom, and provide a copy of the authority to act on behalf of the third party:

_____

When seeking access to personal or health information, you must provide proof of identity in the form of a certified copy of any one of the following documents or other official proof of identity with current address details:

◯ Australian driver's licence (with photograph, signature and current address)

◯ Australian passport

2. Conduct

What is the specific issue or conduct you would like to have reviewed? *('Conduct' can include an action, a decision, or even inaction. For example the 'conduct' in your case might be a decision to refuse you access to your personal information, or the action of disclosing your personal information to another person, or the inaction of a failure to protect your personal information from being inappropriately accessed by someone else.)*

Page 1 of 2

Please tick which of the following describes your concern: *(You can tick more than one)*

- ◯ collection of my personal or health information
- ◯ security or storage of my personal or health information
- ◯ refusal to let me access or find out about my own personal or health information or the accuracy of my personal or health information
- ◯ misuse of my personal or health information or disclosure of my personal or health information without my consent
- ◯ other _____
- ◯ unsure

When did the issue or conduct occur (date)? _____

When did you first become aware of the issue? _____

(Note: You must lodge this application within 6 months of becoming aware of the issue or explain why it has taken more than 6 months to lodge an investigation request)

How has the issue effected you? / What effect might the issue have on you in the future?

3. Remedy

What would you like to see done about the issue? (For example: an apology, a change in policies or practices, training for staff, etc.)

Applicant's lodgment

I understand that the information in this form will be used by Port Authority to process my request for an Internal Review.

I understand that details of my application will be referred to the NSW Privacy Commissioner as required by law, and that the Privacy Commissioner will be kept advised of the progress of the review.

Please post/email this form to: **Attention: Privacy Coordinator**
Post: GPO Box 25, Millers Point, SYDNEY NSW 2001
Email: access2info@portauthoritynsw.com.au |

Page 2 of 2

Port Authority of NSW

PO Box 25

Millers Point NSW 2000

E access2info@portauthoritynsw.com.au

W portauthoritynsw.com.au