1. Purpose of this policy

This Privacy Policy explains how Acute Business Services **[ABS]** collects, holds, uses, discloses and protects personal information **for the purposes of, or in connection with, our obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and AML/CTF Rules**. It also explains how individuals may access and correct their personal information, and how they may make a privacy complaint. Office of the Australian Information Commission **[OAIC]**

This policy is intended to satisfy our obligations to manage personal information in an open and transparent way and to maintain a clearly expressed and up-to-date privacy policy.

---

2. Who this policy applies to

This policy applies to personal information we handle about:

- clients and prospective clients
- beneficial owners, controllers and other related parties
- directors, secretaries, trustees, appointors, partners, officeholders and authorised representatives
- source-of-funds or source-of-wealth contributors where relevant
- staff and contractors **to the extent personal information is handled for AML/CTF personnel due diligence or related AML/CTF purposes**
- other individuals whose personal information we are required to handle to comply with AML/CTF obligations.

If our firm is otherwise exempt from the Privacy Act for some non-AML/CTF activities, this policy applies at least to our personal information handling activities **for AML/CTF purposes**. Small businesses that become reporting entities must comply with the Privacy Act for those AML/CTF-related handling activities.

---

3. Why we collect personal information

We collect personal information where reasonably necessary for one or more of our functions and activities, including to:

- determine whether we can act for a client
- conduct customer due diligence and, where required, enhanced customer due diligence
- identify and verify clients and other relevant individuals
- understand ownership, control and risk associated with a client, matter or transaction
- monitor client relationships and transactions for AML/CTF purposes
- assess and manage money laundering, terrorism financing and proliferation financing risks

- meet our reporting, record-keeping, governance and compliance obligations
- communicate with clients and regulators
- comply with other legal, professional and regulatory obligations applying to our practice.

We take a **data minimisation** approach and seek to limit collection to information that is **reasonably necessary** for our lawful functions and activities. Over-collection is avoided wherever practicable.

---

4. What personal information we may collect

Depending on the engagement, the services provided and the level of AML/CTF risk, we may collect:

Identity and contact details

- full name
- former names or aliases
- date of birth
- residential address and postal address
- email address and telephone number.

Identification and verification details

- passport details
- driver licence details
- other government-issued identity document details
- document type, issue/expiry date, document number and verification outcome
- information used to verify identity electronically.

Business, ownership and control information

- ABN, ACN or other registration details
- company, trust, partnership or other structure details
- shareholding and beneficial ownership details
- directorships, officeholder roles and control information
- trust deed or constituent document information where relevant.

Transaction and engagement information

- information about the nature and purpose of the engagement
- transaction details
- source of funds and, where required, source of wealth information

- payment details and banking information
- records relevant to the designated service being provided.

Risk and compliance information

- sanctions, politically exposed person (PEP) or adverse media screening results
- AML/CTF risk ratings and risk indicators
- internal compliance notes, records of inquiries and escalations
- suspicious matter indicators and related compliance records where permitted by law.

Sensitive information

In limited circumstances, we may collect **sensitive information** where permitted by law and reasonably necessary for our functions or activities, including where collection is required or authorised for AML/CTF compliance or another legal obligation. We will only collect sensitive information where the Privacy Act permits us to do so.

---

5. How we collect personal information

We may collect personal information:

- directly from you
- from identity documents or verification services
- from company, trust or business records supplied to us
- from third parties acting on your behalf, such as authorised representatives, lawyers, bookkeepers, brokers or referrers
- from public registers and reliable independent sources
- from watchlist, sanctions, PEP or other compliance screening providers
- from our website, forms, portals, email, telephone calls and meetings
- from ongoing engagement activity and transaction monitoring.

Where reasonable and practicable, we will collect personal information directly from the individual concerned.

---

6. Is collection required or authorised by law?

In many cases, our collection of personal information is **required or authorised by law**, including under the **AML/CTF Act and AML/CTF Rules**, as well as other taxation, corporate, trust, superannuation or professional regulatory obligations that may apply to the engagement.

If you do not provide certain personal information requested by us, we may be unable to:

- commence or continue acting for you

- provide a designated service
- complete identity verification or customer due diligence
- comply with our legal obligations
- process a transaction or carry out your instructions.

---

7. How we use personal information

We use personal information for the primary purposes for which it was collected, including to:

- verify identity
- conduct initial and ongoing customer due diligence
- carry out enhanced customer due diligence where required
- understand and document client, beneficial owner and transaction risk
- provide accounting, tax, advisory, trust or company and related services
- maintain client records and engagement files
- manage billing, administration, quality assurance and internal audit
- comply with our legal and regulatory obligations
- investigate, manage and respond to fraud, misconduct, compliance concerns or suspicious activity.

We may also use personal information for related secondary purposes where permitted by the Privacy Act, including where you would reasonably expect the use and the use is related to the primary purpose of collection, or where otherwise required or authorised by law.

---

8. How we disclose personal information

We may disclose personal information to:

- our staff, partners, directors and authorised representatives
- related entities within our practice group
- outsourced service providers, including document management, IT, cloud hosting, electronic verification, screening and practice management providers
- professional advisers, auditors and insurers
- banks, financial institutions and payment service providers where relevant
- government agencies, regulators and law enforcement bodies, including **AUSTRAC**, where required or authorised by law
- courts, tribunals or dispute resolution bodies

- other persons where you have consented or where disclosure is otherwise permitted by law.

Our APP 5 collection notices may not include information where doing so would be inconsistent with **tipping-off** restrictions or other legal obligations.

---

9. Overseas disclosure

Some of our third-party service providers may store or process personal information outside Australia (for example, cloud software, identity verification, screening or document management systems). This includes but is not limited to our overseas contractors and service providers such as Xero (New Zealand), Backoffis (Queensland & India), Microsoft & Adobe (USA). Where we are likely to disclose personal information to overseas recipients, we will take reasonable steps required under the Privacy Act, unless an exception applies, including where disclosure is required or authorised by the AML/CTF Act or AML/CTF Rules.

---

10. Security of personal information

We take reasonable technical and organisational steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. These steps may include:

- role-based access controls
- MFA and password protections
- encryption and secure transfer tools
- secure document management systems
- staff confidentiality and privacy training
- controlled physical access
- incident response and data breach procedures
- due diligence and contractual controls for third-party service providers.

We aim to protect personal information throughout its full lifecycle — from collection, to storage and use, to destruction or de-identification.

---

11. Identity documents and copies

Where identity documents are used for verification, we do **not necessarily need to retain scanned copies or photocopies of those documents** for AML/CTF record-keeping purposes. The OAIC has stated that the AML/CTF Act does not require reporting entities to keep copies of identity documents themselves for record-keeping purposes. Instead, it may be sufficient to keep records of the information from the document that is needed to meet AML/CTF obligations, the type of document, what was done to verify identity, and the verification outcome.

Where we do collect copies of identity documents, we will assess whether those copies are still needed and, if not required to be retained for a lawful purpose, we will take reasonable steps to destroy or de-identify them.

---

12. Retention of personal information

We retain personal information for as long as reasonably necessary for the purposes for which it was collected, including to comply with our legal, regulatory, professional and record-keeping obligations. For most AML/CTF obligations, records must generally be retained for **7 years**.

Once personal information is no longer needed for any purpose for which it may be used or disclosed under the Privacy Act, we will take reasonable steps to destroy it or ensure it is de-identified, unless we are required by law or a court/tribunal order to retain it.

---

13. Access to and correction of personal information

You may request access to personal information we hold about you, and you may request correction of inaccurate, out-of-date, incomplete, irrelevant or misleading personal information. We will respond to requests within a reasonable period and in accordance with our obligations under the Privacy Act.

To request access or correction, please contact:

Privacy Officer
Gaye Wade / Practice Manager
Email: gaye@acute.com.au
Phone: (08) 9367 7023

---

14. Privacy complaints

If you believe we have mishandled your personal information, you may make a complaint to us using the contact details above. We will acknowledge and investigate your complaint and aim to respond within a reasonable timeframe. The OAIC recommends organisations should be able to respond to privacy complaints within **30 days**.

If you are not satisfied with our response, you may be able to lodge a complaint with the **OAIC**.

---

15. Changes to this policy

We may update this policy from time to time to reflect changes to our business practices, technology, legal obligations or regulatory guidance. The current version will be made available on our website or on request. Keeping the policy clearly expressed and up to date is part of our APP obligations.