Identitii Limited
ACN 603 107 044
ASX:ID8

Privacy Policy

Owner	Data Protection Officer
Approver	Board of Directors
Reviewer	Information Security Manager
Version	5.0
Last revision date	2026-07-02
Document ID	POL-08
Classification	Public

Introduction

Context

In this Privacy Policy, "Identitii", "we" and "us" mean Identitii Limited (ACN 603 107 044) and its wholly owned Australian subsidiaries, including BNDRY Pty Ltd (ABN 49 678 808 449). It applies to each of these businesses unless that business has published its own privacy policy. If you are a BNDRY customer, or a patron whose identity is verified through a BNDRY customer, this is the policy that governs how your personal information is handled in Australia.

We handle personal information in accordance with the Privacy Act 1988 (Cth) (the Privacy Act) and the Australian Privacy Principles (APPs) in Schedule 1 to that Act. The APPs govern the way we collect, hold, use, disclose, secure and dispose of personal information. A copy of the Privacy Act and the APPs can be obtained from the Office of the Australian Information Commissioner (OAIC) at https://www.oaic.gov.au/.

Where we handle the personal data of individuals located in the European Union or the United Kingdom and the EU General Data Protection Regulation (GDPR) (EU) 2016/679 or the UK GDPR applies to that handling, the additional provisions in the section 'Provisions that apply only under the EU GDPR or UK GDPR' also apply. Those provisions apply only in those cases and create no rights or obligations under the Privacy Act.

Definitions

1. **'Personal information'** has the meaning given in s 6(1) of the Privacy Act: information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether it is recorded in a material form or not. Identification information we handle for identity verification purposes is personal information for the purposes of the Privacy Act, and we protect it accordingly.
2. **'Sensitive information'** has the meaning given in s 6(1) of the Privacy Act and includes information or an opinion about an individual's racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, trade union membership or associations, sexual orientation or practices, criminal record, health information, genetic information, biometric information that is to be used for the purpose of automated biometric verification or biometric identification, and biometric templates. We collect sensitive information only with consent, unless an exception in APP 3.4 applies.
3. **'Personal data'** is the equivalent GDPR term, defined in Article 4(1) of the EU GDPR. In this policy, references to personal information include personal data where the GDPR or UK GDPR applies. When we refer to 'your data' or 'your information', we mean personal information as defined above.

Purpose

The purpose of this policy is to ensure that personal information is handled in a way that respects the privacy rights of individuals and complies with our legal obligations. Identitii is committed to safeguarding the privacy of our clients, employees, partners, website visitors and the individuals whose identities are verified through our services.

Scope

This policy applies to all employees, contractors, website visitors and third-party service providers involved in the handling of personal information on behalf of Identitii.

Objectives

The primary objectives of this policy are to:

1. Protect personal information from misuse, interference, loss, and unauthorised access, modification or disclosure (APP 11.1).
2. Ensure openness and transparency in how we manage personal information (APP 1).
3. Comply with the Privacy Act, the APPs and all other privacy laws and agreements that apply to our activities.

Policy implementation

Responsible parties involved in implementation

Roles and responsibilities incl. responsible authorities for monitoring and enforcement.

Role	Responsibilities
Board of Directors	• Approve and oversee the organisation's privacy policies and data protection strategy. • Provide oversight on risk management, including privacy risks and cybersecurity threats. • Allocate resources for data protection initiatives, training, and technology investments.
CTO	• Ensure technology infrastructure complies with privacy policy requirements. • Implement and maintain systems for data protection and privacy. • Oversee the development of privacy-aware technology solutions.

Information Security Manager	• Monitor compliance with the privacy policy through regular audits and assessments. • Develop and enforce security controls to protect personal data. • Respond to and manage data breaches, ensuring they are reported and mitigated according to policy.
Data Protection Officer (DPO)	• Ensure the organisation's practices comply with relevant privacy laws and regulations. • Conduct privacy impact assessments for new projects and technologies. • Train staff on privacy policies and best practices, and act as the primary contact for privacy-related inquiries and complaints. • Manage data privacy requests and complaints.

Communication and distribution

To ensure effective communication of the policy to relevant stakeholders, the following steps can be taken:

1. Distribution and accessibility:
    a. The policy document should be made available to all relevant stakeholders in a centralised and easily accessible location. This could be achieved by publishing the policy on the organisation's intranet, document management system, or employee portal.
    b. Stakeholders should be notified about the availability of the policy and provided with instructions on how to access it.
    c. A summary of our privacy practices will be made available to our website visitors in the form of a Privacy Statement published on our website.
2. Training and awareness programs:
    a. Conduct training sessions or workshops to educate stakeholders about the policy and its importance.
    b. These sessions can include presentations, interactive discussions, and practical examples to enhance understanding.
    c. Ensure that all employees, including executives, managers, and staff in different roles, attend the training sessions.
    d. It is also important to conduct periodic refresher training to reinforce key policy concepts.

3. Acknowledgement and acceptance:
    a. Require stakeholders to acknowledge their understanding and acceptance of the policy. This can be done through the implementation of an electronic or physical acknowledgement process where stakeholders sign or electronically acknowledge that they have read and understood the policy. This ensures that stakeholders are aware of their responsibilities and are accountable for complying with the policy.
4. Communication channels:
    a. Utilise various communication channels to reinforce the policy's message and updates.
    b. These channels can include internal newsletters, email communications, team meetings, and notice boards.
    c. Regularly communicate updates or changes to the policy, and emphasise the importance of adhering to the policy's guidelines.
5. Ongoing support and guidance:
    a. Establish a designated point of contact to address stakeholders' questions, provide guidance, and offer support related to the policy. This ensures that stakeholders have access to the necessary resources and assistance to comply with the policy.
6. Integration into onboarding process:
    a. Incorporate the policy into the onboarding process for new employees.
    b. During orientation, provide an overview of the policy, explain its relevance to their role, and highlight the expectations for compliance.
    c. Provide access to the policy document and ensure that new employees acknowledge their understanding and acceptance of the policy.
7. Periodic policy review:
    a. Regularly review the policy to ensure its effectiveness and relevance in addressing evolving threats and technologies.
    b. Engage stakeholders in the review process by soliciting feedback and incorporating their insights and experiences into policy updates.
    c. Communicate any changes or revisions to the policy to all stakeholders in a timely manner.

Policy change requests

The process for requesting a change to the policy typically involve the following steps:

1. Identify the need for change
    a. Any stakeholder who identifies the need for a change to the policy should carefully evaluate the rationale behind it. This may include new risks, regulatory changes, technological advancements, or feedback received from employees, auditors, or other relevant sources.
    b. It's important to clearly articulate the reasons for the proposed change.
2. Document the proposed change:
    a. The stakeholder requesting the change should document the proposed modifications to the policy. This includes detailing the specific sections or clauses that require revision, addition, or removal, along with a clear explanation of the desired changes and the expected outcomes.

3. Impact assessment:
    a. The proposed change should undergo an impact assessment to evaluate its potential consequences. This assessment may involve considering the impact on existing processes, procedures, technical controls, resources, and compliance requirements.
    b. It's crucial to assess both the positive and negative implications of the change.
4. Consultation and collaboration:
    a. The stakeholder should engage in consultation and collaboration with relevant parties to gather input and feedback. This may include discussions with members of the information security team, legal counsel, HR, risk management personnel, and other subject matter experts. Their expertise and perspectives can help evaluate the viability and effectiveness of the proposed change.
5. Review and approval process:
    a. The proposed change should undergo a formal review process, which may involve a designated committee or a specific individual responsible for policy management.
    b. The review process evaluates the proposed change in light of the organisation's goals, compliance requirements, and overall risk posture.
    c. The approval authority assesses the proposed change and decides whether to approve, reject, or request further modifications.
6. Communication and documentation:
    a. Once the change is approved, it should be communicated to all relevant stakeholders. This includes updating the policy document with the revised sections or incorporating an addendum to the existing policy.
    b. The updated policy should be made easily accessible to all stakeholders through the organisation's established communication channels.
7. Training and awareness:
    a. Conduct training or awareness sessions to educate employees about the revised policy. This ensures that all individuals affected by the change are aware of their new obligations and understand the reasons behind the modification.
    b. Training sessions may include explanations of the change, examples of its practical application, and clarification of any questions or concerns raised by employees.
8. Implementation and monitoring:
    a. The revised policy should be implemented and enforced across the organisation.
    b. Ongoing monitoring and compliance assessments should be conducted to ensure adherence to the updated policy
    c. Any deviations or non-compliance should be addressed through appropriate corrective actions.

Policy exception process

Implementing a policy exception requires a careful evaluation and approval process to ensure that exceptions are justified, properly managed, and do not compromise the organisation. The process for implementing a policy exception typically involves the following steps:

1. Identify the need for an exception:
    a. A stakeholder or individual within the organisation identifies a situation or circumstance that warrants an exception to a specific policy.
    b. The need for the exception must be clearly defined and supported by valid reasons, such as business requirements, technical limitations, or legal or regulatory obligations.
2. Documentation of the exception request:
    a. The stakeholder requesting the exception should document the details of the exception request. This includes specifying the policy or control from which the exception is sought, describing the reason for the exception, and providing any supporting evidence or documentation.
3. Evaluation and risk assessment:
    a. The exception request undergoes an evaluation and risk assessment process. This involves assessing the potential impact of granting the exception on the organisation's security, compliance, and overall risk posture.
    b. The evaluation should consider the severity of the identified risk, available mitigating controls, and alternative solutions to address the situation.
4. Review and approval process:
    a. The exception request is reviewed by the appropriate authority or committee responsible for policy governance and compliance. This may involve the information security team, HR, risk management personnel, legal counsel, or other relevant stakeholders.
    b. The review assesses the justification, feasibility, and acceptability of the requested exception.
    c. The approval authority makes a decision to approve, reject, or request further modifications to the exception request.
5. Documentation and tracking:
    a. Once the exception is approved, it should be properly documented, including the justification for the exception, the approval details, and any conditions or limitations associated with the exception. This documentation helps ensure transparency, accountability, and auditability.
    b. The exception request and its approval status should be tracked in a centralised repository or system for future reference and reporting.
6. Communication and awareness:
    a. The approved exception should be communicated to the relevant stakeholders who are affected by the exception. This includes notifying individuals responsible for implementing or enforcing the policy, as well as any other personnel who may be impacted by the exception.
    b. It's essential to ensure that all affected parties understand the scope, limitations, and duration of the exception.

7. Monitoring and review:
    a. The exception should be periodically reviewed to assess its ongoing relevance and validity. This includes monitoring the associated risks, evaluating any changes in the organisation's environment, and reassessing the need for the exception.
    b. If circumstances change, the exception may be modified, extended, or revoked based on the reassessment results.
8. Reporting and accountability:
    a. The exception process should include reporting mechanisms to ensure proper oversight and accountability. This may involve regular reporting to senior management, the board of directors, or other governing bodies to provide visibility into the exceptions granted and their associated risks.

Policy requirements

Requirements applicable to all staff

1. Adhere to this policy and related procedures.
2. Report any data breaches or privacy concerns to the Data Protection Officer immediately.
3. Ensure that personal information is only accessed and used for legitimate business purposes.

Requirements applicable to line managers

1. Ensure their teams are aware of and comply with this policy.
2. Facilitate privacy training and awareness programs.
3. Report any issues related to privacy compliance to the Data Protection Officer.

Principles

Open and transparent management of personal information

APP 1 requires us to manage personal information in an open and transparent way. This policy is clearly expressed, kept up to date (APP 1.3), and sets out the matters required by APP 1.4: the kinds of personal information we collect and hold, how we collect and hold it, the purposes for which we collect, hold, use and disclose it, how you can access your personal information and seek correction, how you can complain and how we deal with complaints, whether we are likely to disclose personal information to overseas recipients, and the countries in which those recipients are likely to be located.

Data minimisation and accuracy

Data minimisation

We collect personal information (other than sensitive information) only where it is reasonably necessary for one or more of our functions or activities (APP 3.2), and we collect it by lawful and fair means (APP 3.5). We collect personal information from the individual concerned unless it is unreasonable or impracticable to do so or another exception applies (APP 3.6). Our practices include:

1. Personal information is collected for explicit, legitimate purposes and handled in ways compatible with those purposes.
2. We ensure the information we collect is adequate, relevant and limited to what is necessary, and we review the information we hold regularly to confirm its relevance and necessity.
3. Our collection methods are designed to gather only the information needed for each specific purpose, avoiding the collection of excessive or irrelevant data.

Data accuracy

We take reasonable steps to ensure the personal information we collect is accurate, up to date and complete (APP 10.1), and that the personal information we use or disclose is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure (APP 10.2). Our practices include:

1. Validating information at the point of collection and reviewing it periodically.
2. Providing mechanisms for individuals to update or correct their personal information by contacting privacy@identitii.com. Correction requests are handled promptly.
3. Technical and organisational measures to maintain the integrity of information through its lifecycle, including validation checks, user confirmation steps and validation against authoritative sources.

Anonymity and pseudonymity

Where lawful and practicable, you have the option of dealing with us anonymously or under a pseudonym (APP 2). This may apply to low-risk interactions such as general enquiries or optional feedback. In most cases it is impracticable for us to deal with individuals who have not identified themselves, particularly where identity verification is required to deliver our services, to comply with regulatory obligations including the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act), or to manage risk appropriately.

What data we collect

The kinds of personal information we collect and hold depend on your relationship with us as a website visitor, employee, contractor, customer, job applicant or individual undergoing identity verification. If you are unsure what personal information we collect based on your relationship with us, or would like to request access to or correction of your information, contact us at privacy@identitii.com.

Data categories

1. Personal information: names, addresses, email addresses, phone numbers, job titles, employment history, professional qualifications.
2. Government identification: driver licence, passport, visa, citizenship certificate, registration by descent certificate, birth certificate, marriage certificate, death certificate, change of name certificate, Medicare card, Centrelink concession card, ImmiCard, aviation security identification card (ASIC), maritime security identification card (MSIC).
3. Device information: IP addresses, browser types and versions, operating systems.
4. Cookie data: necessary, functional, analytics, performance and advertisement cookies.
5. Customer support: support queries, emails, application logs.
6. Marketing communications: subscription preferences, marketing preferences, engagement with marketing emails.
7. Financial information: bank details, invoices, billing addresses.
8. Social media: publicly available profile information, interactions with our accounts, content you share with us, engagement data, demographic information you have made public, and device information.
9. Feedback, complaints and survey responses.
10. Information available from public sources.

Children's data

Our services are not specifically targeted at children. However, if any part of our platform is likely to be accessed by individuals under the age of 18, we will comply with the Children's Online Privacy Code (COPC) once it is issued by the Office of the Australian Information Commissioner (OAIC).

This includes implementing age-appropriate consent mechanisms, limiting profiling, and ensuring that privacy is protected by default for young users. If it is not practicable or reasonable for us to assess the capacity of individuals under 18 on a case-by-case basis, we will presume that individuals aged 15 or over have the capacity to consent unless there is reason to believe otherwise. Individuals under the age of 15 are presumed not to have capacity to consent, and we will instead seek consent from a parent or legal guardian, where applicable.

We also reserve the right to decline access to our services for individuals under the age of 15, where we are unable to obtain appropriate parental or guardian consent or where it would not be appropriate to deliver the service to a child.

Consent for processing personal and sensitive data

When we rely on consent

We obtain your consent where:

- we collect sensitive information, including biometric information and biometric templates, unless an exception in APP 3.4 applies (for example, where collection is required or authorised by or under an Australian law, or a permitted general situation exists)
- we send you marketing communications, including newsletters, product updates and promotional offers (APP 7)
- we verify your identity against official records (see 'Consent for identity verification' below)
- we handle the personal information of a child and consent from a parent or guardian is required
- we use cookies and similar technologies that are not strictly necessary for our websites or applications to function

Australian requirements for consent

Consent must be voluntary, informed, current and specific, and given by a person with the capacity to do so. For sensitive information, we require express consent and collect it only where the collection is also reasonably necessary for one or more of our functions or activities (APP 3.3), unless an APP 3.4 exception applies. We record consent so that we can demonstrate it was validly obtained.

GDPR requirements for valid consent

Where we rely on consent under the EU or UK GDPR:

- Consent must be freely given, specific, informed, and unambiguous. This means individuals are given a genuine choice and are not coerced or misled.
- For sensitive personal data, consent must be explicit (Art. 9(2)(a)). This requires a clear, affirmative statement (not implied consent or pre-ticked boxes).
- Individuals must be informed of:
    - The identity of the data controller.
    - The specific purposes of processing.
    - Their right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before withdrawal.

We maintain records of consent in accordance with the accountability principle under Article 5(2) of the GDPR.

Consent for identity verification

Where we or our customers verify an individual's identity by checking their document details against official records held by document issuers or government record holders, we require express consent from that individual before any verification request is initiated.

This consent is obtained separately from any other agreement or terms of service and is never bundled with other consents. The individual is clearly informed that their identification information will be collected, used and disclosed for the purpose of verifying their identity, and that the process may involve the use of third-party systems and service providers. Consent is obtained before any verification request is submitted.

More information can be found at https://www.bndry.net/legals/identity-verification.

Withdrawal of consent

You have the right to withdraw your consent at any time. We make this easy by including unsubscribe links in all marketing emails, providing cookie preference controls on our website, and accepting withdrawal requests at privacy@identitii.com. Upon withdrawal we will stop handling your personal information for the relevant purpose unless another lawful basis exists. Withdrawal does not affect handling that lawfully occurred before the consent was withdrawn.

Exceptions to consent

We may collect or handle sensitive information without consent where an exception in APP 3.4 or GDPR Article 9(2)(b–j) applies, including where the collection is required or authorised by or under an Australian law (for example the AML/CTF Act) or a court or tribunal order, where a permitted general situation exists (for example lessening or preventing a serious threat to life, health or safety, or taking appropriate action in relation to suspected unlawful activity or serious misconduct), or where a permitted health situation exists. In these cases we assess whether the handling is proportionate and necessary and ensure additional safeguards are in place.

How we collect your data

Direct collection methods

We collect personal information directly from you when you: submit an enquiry form on our website; sign a contract for our products or services; complete a survey or provide feedback; use or view our website (via your IP address and cookies, only with your consent except for strictly necessary cookies); contact our customer support team; register for or attend an event we host; or voluntarily provide personal information in any other manner, including in conversations, shared documents, online forms or uploads.

Indirect collection methods

We may also receive personal information from third parties, including: business partners or service providers who collect data on our behalf; our customers or integration partners who collect personal information directly from individuals in the course of using our services and provide it to us as part of service delivery or regulatory reporting; affiliates or subsidiaries as part of collaborative business operations; publicly accessible sources such as public databases and industry directories; and referrals. We handle all indirectly collected personal information in accordance with this policy and, where you may be unaware of the collection, we take reasonable steps to notify you of the matters in APP 5.2 or to ensure you are aware of them.

Unsolicited personal information

If we receive unsolicited personal information, we promptly assess whether we could have collected it under APP 3. If we could not have collected it lawfully and there is no legal requirement to retain it, we take all reasonable steps to securely destroy or de-identify it as soon as practicable (APP 4). We retain unsolicited personal information only where there is a clear and lawful purpose for doing so.

Cookies

Our website uses cookies to enhance your experience, analyse site traffic, and serve tailored advertisements. Upon your first visit, you will be presented with a cookie consent banner that clearly outlines the types of cookies we use and their purposes. The cookie banner gives you the option for granular opt-in consent. With the exception of the cookie consent banner, which is required to record your consent, no cookies are loaded prior to your consent.

What are cookies?

Cookies are small data files that are placed on your computer or mobile device when you visit a website, mobile app or use an online product. Cookies are widely used to facilitate and help to make the interaction between users and websites, mobile apps and online products faster and easier, as well as to provide reporting information.

How to manage your cookies

Most web browsers allow you to block or delete cookies, including those set by third-party subdomains, through your browser settings, and some third-party services provide their own tools for managing cookie preferences. Visit the privacy policy or cookie settings page of the third-party service for more information. If you elect not to activate a cookie or to later disable cookies, your ability to use some features or areas of our website can be impacted.

Information about opting out of targeted advertising can be found at:

- http://www.youronlinechoices.eu/ if located in the European Union.
- https://www.oaic.gov.au/privacy/your-privacy-rights/social-media-and-online-privacy/targeted-online-marketing if located in Australia.

In addition, certain third party advertising networks permit users to opt out of or customise preferences associated with your internet browsing.

How do we use cookies?

We use various technologies to collect information, and this includes sending cookies to your computer or mobile device. Cookies help us to improve our services and your experience, see which areas and features of our services are popular, count visits, and distinguish between visitors. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. Our website will use cookies to analyse website traffic and help us provide a better website visitor experience. In addition, cookies are used to serve relevant ads to website visitors through third-party services. These ads can appear on this website or other websites you visit.

What cookies do we use?

In general, there are three different ways to classify cookies: their purpose, their duration, and their provenance. We use the following cookies on our website and subdomains.

1. Purpose
    a. Necessary – Essential for the website to function properly, such as enabling security features and allowing users to navigate the site.
    b. Functional – Enhance usability by remembering preferences and customisations, such as language settings.
    c. Analytics – Collect anonymous data on user interactions and website performance to improve user experience.
    d. Performance – Monitor and optimise website performance, ensuring fast load times and smooth navigation.
    e. Advertisement – Track browsing behaviour to deliver personalised ads and limit ad frequency.
2. Duration
    a. Session cookies – These cookies are intended to persist only for the duration of your browsing session and are typically deleted when the browser is closed. However, some modern browsers (e.g. Chrome, Firefox) may retain session cookies if session restore is enabled or the browser is configured to reopen tabs after restart.
    b. Persistent cookies — This category encompasses all cookies that remain on your hard drive until you erase them or your browser does, depending on the cookie's expiration date. All persistent cookies have an expiration date written into their code, but their duration can vary.
3. Provenance
    a. First-party cookies — As the name implies, first-party cookies are put on your device directly by our website.
    b. Third-party cookies — These are the cookies that are placed on your device, not by our website, but by a third-party like an advertiser or an analytic system.

Third-party hosting cookies

Our website will have links to other websites not owned or controlled by us. These links are meant for your convenience only. Links to third-party websites do not constitute sponsorship, endorsement, or approval of these websites. Please be aware that we are not responsible for the privacy practices of such other websites. We encourage our users to be aware, when they

leave our website, to read the privacy statements of each and every website that collects personally identifiable information.

Some subdomains of our website are controlled by us but hosted by third-party service providers, including, but not limited to:

- docs.bndry.net
- investorhub.identitii.com
- status.bndry.net
- support.bndry.net
- trust.bndry.net

This is made possible through the use of CNAME (canonical name) records. A CNAME record acts like a forwarding address. Instead of pointing directly to a location (an IP address), it points to another domain name. This other domain name then points to the final location.
For example, if you visited example.identitii.com, a CNAME record would direct your browser to example.com, which then serves the content for example.identitii.com.

When you access subdomains, some requests are managed by our third-party partner's servers. They will set their own cookies and manage your data according to their privacy practices. This means that these subdomains use cookies that are set and managed by the third-party service providers, and your data will be handled according to the privacy policies of these third-party providers. We recommend that you review the privacy policies of these third-party service providers to understand their practices regarding cookies and personal data.

Cookie consent
Our cookie banner allows you to give granular consent by category. Except for strictly necessary cookies used to record your preferences, no cookies are activated until you have made a clear, affirmative choice. By selecting your cookie preferences on our cookie consent banner, you consent to our use of cookies as described in this policy. You can change your preferences or withdraw consent at any time through the cookie settings link available on our website.

How we store and retain your data

Identitii maintains a standard outlining how we manage data privacy and protection, the roles and responsibilities of staff involved in data management, and a data retention schedule specifying the minimum retention period for different classes of records and the actions taken at the end of the retention period.

We retain personal information only for as long as it is needed for the purposes for which it was collected, or as required by law. We review stored information regularly to confirm it remains accurate, up to date and necessary. When personal information is no longer needed for any purpose for which it may be used or disclosed, and we are not legally required to retain it, we take reasonable steps to destroy it or ensure it is de-identified (APP 11.2) and Article 5(1)(e) of the GDPR.

How we secure your data

Security controls

We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure (APP 11.1). Our technical and organisational measures include:

- Encryption of personal information in transit and at rest using industry-standard protocols (TLS 1.2 or higher in transit, AES-256 at rest)
- Access to personal information strictly limited to authorised personnel on the principle of least privilege, with multi-factor authentication enforced for internal systems handling personal information
- Firewalls, intrusion detection and prevention systems, and endpoint security to protect against cyber threats
- Secure development practices, including regular security testing and code reviews
- Third-party due diligence on vendors handling personal information

Employee training and awareness

- All employees undergo mandatory cybersecurity and privacy training on hiring and annual refresher training.
- Employees must report any suspected data breaches or security incidents to the Information Security Manager and the Data Protection Officer.

Compliance and auditing

- We conduct internal and third-party security audits to assess compliance with regulatory requirements and identify areas for improvement.
- We perform risk assessments at least annually to evaluate emerging security threats and adjust our security posture.
- We maintain our program against the Privacy Act and the APPs and against recognised information security frameworks such as ISO 27001 and SOC 2, and against the GDPR where it applies.

Security monitoring and assessment

- We continuously monitor for security threats, suspicious activity and potential data breaches using automated security event monitoring.
- We conduct penetration tests at least annually to identify and mitigate vulnerabilities in our infrastructure.

Data breach response

If we suspect a data breach involving personal information, we follow this process:

1. **Containment and remediation:** take urgent action to contain the breach and mitigate risks, and implement technical and administrative controls to prevent recurrence.
2. **Assessment:** where we suspect an eligible data breach may have occurred, we carry out a reasonable and expeditious assessment, completed within a maximum of 30 days (Privacy Act s 26WH). An eligible data breach is unauthorised access to, unauthorised disclosure of, or loss of personal information that a reasonable person would conclude is likely to result in serious harm to any individual to whom the information relates.
3. **Notification:** if we form reasonable grounds to believe an eligible data breach has occurred, we prepare a statement and notify the Office of the Australian Information Commissioner and affected individuals as soon as practicable. If it is impracticable to notify each individual directly, we publish the statement on our website and take reasonable steps to publicise it.
4. **Customer notification:** where we process personal information on behalf of a customer, we notify that customer without undue delay after becoming aware of a security incident affecting their personal information, and in any event within 48 hours, in accordance with the applicable data processing agreement.
5. **Post-incident review:** conduct a root cause analysis, implement corrective measures, and report findings to senior management and, where required, to regulators.

The requirement to notify a supervisory authority within 72 hours applies only where the EU GDPR or UK GDPR applies to the personal data involved; see the section 'Provisions that apply only under the EU GDPR or UK GDPR'.

If you suspect a data breach involving your personal data, please contact us immediately at privacy@identitii.com.

How we use your data

We use and disclose personal information for the primary purpose for which it was collected, and for secondary purposes only where you have consented, where you would reasonably expect the use or disclosure and it is related (or, for sensitive information, directly related) to the primary purpose, where it is required or authorised by or under an Australian law or a court or tribunal order, or where another APP 6.2 exception applies. Our purposes and the basis for each under the APPs are:

Purpose	Basis under the APPs
Provision of services: regulatory reporting, customer onboarding and due diligence, customer risk management, identity verification and payment investigation services	Primary purpose of collection (APP 6.1); performance of our contract with you or your organisation
Compliance and legal obligations, including obligations under the AML/CTF Act	Required or authorised by or under an Australian law (APP 3.4(a), APP 6.2(b))
Customer support and service updates, including maintenance, outage and release notices	Primary purpose, or a related secondary purpose you would reasonably expect (APP 6.2(a))
Internal operations and security: protecting our legal rights, property, information assets, customers and third parties	Related secondary purpose you would reasonably expect (APP 6.2(a)); enforcement and misconduct exceptions where applicable
Financial transactions: payments, billing and invoicing	Primary purpose of collection (APP 6.1)
Investor relations: ASX announcements, annual reports and disclosure obligations	Required or authorised by law, including the Corporations Act 2001 (Cth) and ASX Listing Rules (APP 6.2(b))
Recruitment: processing applications, assessing qualifications and verifying information	Collection reasonably necessary for our functions or activities (APP 3.2); primary purpose (APP 6.1)
Verifying your identity when responding to access, correction or other privacy requests	Required or authorised by law (APP 12, APP 13)
Website analytics	Consent, given through our cookie banner
Marketing communications	Consent (APP 7); you can opt out at any time
Event registration and participation	Consent; primary purpose of collection

Automated decision-making and profiling

In some areas of our operations we use profiling and automated decision making to enhance security, meet regulatory obligations and improve service efficiency. These processes identify risk, verify identities and detect fraud using behavioural patterns, system events and user attributes. Contexts where an automated process could significantly affect an individual include:

- fraud detection and prevention, where automated detection of suspicious behaviour may result in temporary or permanent service restrictions
- security operations, where a user may be locked out after triggering anomaly detection rules
- identity verification for know your customer and AML/CTF purposes, where failure of automated checks may delay onboarding or require alternative verification
- access management, where access may be denied automatically based on identity or device anomalies

We ensure meaningful human involvement in automated decision making that may significantly affect you. This includes review by trained personnel, escalation to a privacy or risk officer if concerns are raised, and documented outcomes to support fairness, transparency and accountability. You can ask us to review a decision, express your point of view and receive an explanation of how the decision was made by contacting privacy@identitii.com.

The description above sets out our use of computer programs to make, or to do things substantially and directly related to making, decisions that could reasonably be expected to significantly affect your rights or interests, and the kinds of personal information used in those decisions, consistent with APP 1.7, which commences 10 December 2026. The rights that apply to solely automated decisions under GDPR Article 22 arise only where the GDPR or UK GDPR applies; see the GDPR section below.

Use of government-related identifiers

We do not adopt, use or disclose government-related identifiers, such as Medicare numbers, Tax File Numbers or other identifiers assigned by an Australian Government agency, as our own identifier of an individual (APP 9.1). We use or disclose such identifiers only where it is (APP 9.2):

1. Reasonably necessary to verify the identity of the individual for the purposes of our activities or functions;
2. Reasonably necessary to fulfil our obligations to an Australian Government agency or a State or Territory authority; or
3. Required or authorised by or under an Australian law or a court or tribunal order.

Identity documents such as driver licences and passports contain government-related identifiers. We apply the same restrictions to the identifiers they contain: limited use, no adoption as our own identifier, and no disclosure beyond what the APPs permit. Tax file number information is handled in accordance with the Privacy (Tax File Number) Rule 2015, which applies in addition to the APPs.

Where we verify identity documents against official records held by document issuers or government record holders, we handle all identifier data and verification results in strict accordance with our participation agreements and applicable privacy laws. This includes ensuring that:

1. Access to identity verification services is limited to authorised personnel and used exclusively for the purpose of verifying the identity of an individual who has provided their express consent to that verification;
2. Identification information is not collected, stored or used for any purpose other than what is strictly necessary to perform the identity verification requested;
3. Verification results are recorded and auditable to support compliance with our legal and contractual obligations;
4. Information obtained through the verification process is never used for commercial profiling, marketing, advertising or the provision of information services;
5. Information obtained from the verification process, including any results, is used and disclosed only for providing the verification service and meeting our legal and contractual obligations; and
6. Personal information obtained through the verification process is used and disclosed only to the extent strictly necessary for legitimate identity verification purposes.

For the avoidance of doubt, identification information obtained for identity verification purposes will never be used or disclosed for the purpose of: creating a data profile of the individual whose identity is being verified, including tracking the individual's behaviour whether online or offline; offering to supply goods or services to that individual; advertising or promoting goods or services; enabling any other person or entity to offer, supply, advertise or promote goods or services; or conducting market research.

Information provided to individuals undergoing identity verification

Where an individual's identity is verified using official records, we ensure the following information is made available to that individual before the verification takes place:

1. How we and our customers use the identity verification service, including that the individual's information will be checked against official records held by document issuers or government record holders;
2. That the verification process may involve the use of third-party systems and service providers, and a description of the categories of those service providers;
3. The legal obligations we and our customers have in relation to the collection of the individual's identification information;
4. The individual's rights in relation to the collection of their identification information;
5. The consequences if the individual declines to provide consent;
6. Where the individual can obtain information about making complaints relating to the collection, use and disclosure of their identification information; and
7. Where the individual can obtain information about the operation and management of the verification service by the relevant government administrator.

Disclosure of your data

Internal disclosure

We disclose your data to our employees, officers, insurers, professional advisers, agents, suppliers or subcontractors as reasonably necessary for the purposes set out in this policy.

Third-party vendor disclosure

Your data is supplied to a third-party vendor only when it is required for the delivery of our services. When we disclose your data to third parties, we require them to handle it consistently with this policy and the APPs, usually through enforceable contractual terms. A list of third parties and the nature of the data shared is available at https://trust.bndry.net/subprocessors.

Cross-border disclosure

General corporate information

Personal information collected for our corporate functions, such as marketing, recruitment, customer support and website analytics, may be disclosed to or accessed by service providers located in the United States, the Philippines and the European Union. If disclosure to additional countries is anticipated, we will update this policy (APP 1.4(f) and (g)).

Before we disclose personal information to an overseas recipient, we take reasonable steps to ensure the recipient does not breach the APPs in relation to that information, usually through enforceable contractual terms, and we remain accountable for the acts and practices of the overseas recipient under APP 8.1 and s 16C of the Privacy Act unless an exception in APP 8.2 applies.

As at the date of this policy, no country has been prescribed by regulation for the purposes of the prescribed country exception in APP 8.3, so we place no reliance on any Australian Government country list.

Identification information handled through our identity verification service

Identification information and verification results used to provide identity verification are stored and accessed only within Australia. The systems used to deliver the verification service are located in Australia, operated in a dedicated environment controlled by us, and the management and control of the service is conducted in Australia. Overseas access to this information occurs only where it has been authorised in writing under our participation agreements, and any overseas personnel involved must comply with the APPs in respect of all personal information they receive. This information is not held or processed in the United States, the Philippines or the European Union.

Where the EU GDPR or UK GDPR applies to a transfer of personal data, the additional transfer safeguards described in the GDPR section of this policy also apply.

Data subject requests

We handle requests to access, correct or otherwise deal with personal information in accordance with the Privacy Act and, where applicable, the GDPR. Requests should be submitted to privacy@identitii.com. On receipt we promptly log and acknowledge the request and verify the requestor's identity, then assess the request, collect and review the relevant information, and prepare a clear response. We may decline a request in the limited circumstances set out in the relevant legislation, and if we do, we provide written reasons and information about how to complain. We ensure secure delivery of the response and maintain records of requests and outcomes.

Government data requests

At times we need to disclose personal information to comply with legal requirements. As a foundational principle, we will disclose personal information in response to a government data request only where we are under a compelling legal obligation, or where, considering the nature, context, purposes, scope and urgency of the request and the privacy rights of affected individuals, there is an imminent risk of serious harm warranting compliance.

Unless legally prohibited or facing an imminent risk of serious harm, we notify and consult with competent privacy regulators and, if we are processing personal information on behalf of a customer, that customer, before responding. We strictly prohibit any transfer of personal information to a requesting authority that is massive, disproportionate and indiscriminate, going beyond what is necessary in a democratic society. We warrant that we have never purposefully created or maintained back doors or business processes designed to facilitate mass and indiscriminate government access to personal information, in transit or at rest, and any person who becomes aware of such a mechanism must promptly notify the Data Protection Officer.

Sale, transfer, or change of control

In the event of a change of control in our business or a sale or transfer of business assets, we reserve the right to transfer our user databases, including personal information contained in them, to the extent permitted by law. Information is disclosed to a potential purchaser only under an agreement to maintain confidentiality, in good faith, and only where required by those circumstances.

Your rights under the Privacy Act

Access to your personal information

You have the right to request access to the personal information we hold about you (APP 12). We respond within a reasonable period after the request is made, generally within 30 days, and give access in the manner you request where it is reasonable and practicable to do so (APP 12.4 and 12.5). We do not charge for making a request, and any charge for giving access will not be excessive and will not apply to the making of the request (APP 12.7 and 12.8).

We may refuse access only in the circumstances set out in APP 12.3, for example where giving access would have an unreasonable impact on the privacy of others or would be unlawful. If we refuse access, or refuse to give access in the manner requested, we give you written reasons, the mechanisms available to complain about the refusal, and, where reasonable, access by other means (APP 12.9 and 12.10).

Correction of your personal information

You have the right to request correction of personal information that is inaccurate, out of date, incomplete, irrelevant or misleading (APP 13). We respond within a reasonable period, generally within 30 days, and we do not charge for making a correction request or for correcting information (APP 13.5). If we have previously disclosed the information to another APP entity and you ask us to, we take reasonable steps to notify that entity of the correction (APP 13.2).

If we refuse to correct the information, we give you written reasons and the available complaint mechanisms, and, if you ask, we take reasonable steps to associate a statement with the information noting that you consider it inaccurate, out of date, incomplete, irrelevant or misleading (APP 13.3 and 13.4).

Direct marketing

Where we use or disclose personal information for direct marketing, we do so only with your consent or where you would reasonably expect it, and every marketing communication contains a prominent, simple means of opting out (APP 7). You can opt out at any time, and you can ask us to identify the source of the information we used (APP 7.6). We never use sensitive information for direct marketing without your express consent. Our electronic marketing complies with the Spam Act 2003 (Cth) and any telemarketing complies with the Do Not Call Register Act 2006 (Cth).

Dealing with us anonymously

Where it is lawful and practicable, you have the option of dealing with us anonymously or under a pseudonym (APP 2). This is generally impracticable where we verify identity or meet AML/CTF obligations; see the Anonymity and pseudonymity section above. You can also withdraw any consent you have given at any time; see Withdrawal of consent.

Complaints

If you believe we have interfered with your privacy or breached the APPs, you can lodge a complaint with us by email to privacy@identitii.com or by mail to our registered address: C/- Boardroom Pty Limited, Level 8, 210 George Street, Sydney NSW 2000. When making a complaint, please identify yourself, provide any relevant reference numbers, describe the matter and why you consider your personal information was mishandled, tell us what you would like us to do to resolve it, and provide contact details. We acknowledge complaints promptly, investigate them internally, and aim to provide a written response within 30 days. We suggest you keep a record of your complaint and our responses.

If you feel that we have not addressed your concern in a satisfactory manner, you have the right to lodge a complaint with the relevant supervisory data authority:

- **Office of the Australian Information Commissioner (OAIC)**
  - Website: https://www.oaic.gov.au/
  - Contact details: https://www.oaic.gov.au/contact-us
  - Make a complaint: https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us
- **Relevant EU Data Supervisory Authority**
  - Contact details: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en
- **UK Information Commissioner's Office (ICO)**
  - Website: https://ico.org.uk
  - Context details: https://ico.org.uk/global/contact-us/
  - Make a complaint: https://ico.org.uk/make-a-complaint/

Right to sue for serious invasions of privacy

Individuals in Australia may have the right to take legal action under a statutory tort if they believe their privacy has been seriously invaded. This right applies where a person has suffered harm due to intentional or reckless conduct, such as the unauthorised disclosure, misuse, or interference with their personal information in a manner that would be highly offensive to a reasonable person.

This right is separate from our internal complaints process and from the oversight of the Office of the Australian Information Commissioner (OAIC). If you believe your privacy has been seriously breached in this way, you may seek independent legal advice about your options for initiating civil proceedings.

Provisions that apply only under the EU GDPR or UK GDPR

The provisions in this section apply only where we handle the personal data of individuals located in the European Union or the United Kingdom and the EU GDPR or UK GDPR applies to that handling. They create no rights or obligations under the Australian Privacy Act.

Legal bases for processing

Where the GDPR applies, we process personal data under Article 6 on the basis of: performance of a contract (service delivery, customer support, billing); compliance with a legal obligation (regulatory reporting, responding to data subject requests); our legitimate interests (website analytics, service updates, investor relations, recruitment, security and fraud prevention), balanced against your rights and freedoms; and consent (marketing, event registration, non-essential cookies). Special categories of personal data are processed only with explicit consent under Article 9(2)(a) or where another Article 9(2) condition applies.

Valid consent

Where we rely on consent under the GDPR, it is freely given, specific, informed and unambiguous, obtained through a clear affirmative act rather than pre-ticked boxes or implied acceptance. You are informed of the identity of the controller, the purposes of processing and your right to withdraw consent at any time without affecting the lawfulness of prior processing. We keep records of consent in accordance with the accountability principle in Article 5(2).

International transfers

Where we transfer personal data from the European Economic Area or the United Kingdom to a third country, we rely on an adequacy decision or, where none applies, on Standard Contractual Clauses approved by the European Commission, supported by a transfer impact assessment considering the nature and sensitivity of the data, the circumstances of the transfer, the legal framework of the destination country and any supplementary safeguards. We conduct data protection impact assessments for processing likely to result in a high risk to individuals' rights and freedoms. We place no reliance on Binding Corporate Rules. In limited cases we rely on other lawful transfer mechanisms such as your explicit consent or necessity for the performance of a contract.

Personal data breaches

Where the GDPR or UK GDPR applies, we notify the relevant supervisory authority of a personal data breach without undue delay and, where feasible, within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to individuals' rights and freedoms (Article 33). Where a breach is likely to result in a high risk to individuals, we also communicate it to the affected individuals without undue delay (Article 34).

Your GDPR rights

- **Access (Article 15):** confirmation of processing, a copy of your personal data and supplementary information.
- **Rectification (Article 16):** correction of inaccurate or incomplete personal data.
- **Erasure (Article 17):** deletion in certain circumstances. We may refuse where processing is necessary for freedom of expression and information, compliance with a

legal obligation or a task in the public interest, public health, archiving or research purposes, or the establishment, exercise or defence of legal claims.

- **Restriction of processing (Article 18):** where you contest accuracy, processing is unlawful and you prefer restriction to deletion, we no longer need the data but you need it for legal claims, or you have objected and verification is pending.
- **Data portability (Article 20):** a structured, commonly used, machine readable copy of your personal data, and transmission to another controller where technically feasible.
- **Objection (Article 21):** to direct marketing at any time, and to processing based on legitimate interests unless we demonstrate compelling legitimate grounds that override your rights.
- **Automated decision making (Article 22):** the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal or similarly significant effects, and the rights to human intervention, to express your point of view and to contest the decision.
- **Notification (Article 19):** we notify recipients of your personal data of any rectification, erasure or restriction, unless this is impossible or involves disproportionate effort. We do not charge a fee to process requests unless a request is manifestly unfounded or excessive, in which case we may charge a reasonable administrative fee or refuse the request (Article 12(5)).

Supervisory authorities

If you are in the EU, you can lodge a complaint with your local supervisory authority; member authorities are listed at https://www.edpb.europa.eu/about-edpb/about-edpb/members_en. If you are in the UK, you can complain to the Information Commissioner's Office at https://ico.org.uk/make-a-complaint/.

How to exercise your rights

To exercise any of your rights, contact us by email at privacy@identitii.com or by mail to our registered address: C/- Boardroom Pty Limited, Level 8, 210 George Street, Sydney NSW 2000. We will respond within 30 days. If we refuse a request, we will provide a written explanation of the reasons and your options for further recourse.

If you would like to give us feedback about our privacy practices, please include as much detail as possible and send it to privacy@identitii.com.

Changes to our privacy policy

We update this policy to reflect changes in our practices or for operational, legal or regulatory reasons. Modifications are effective when posted on our website. We encourage you to review the policy periodically. If we make material changes, we will notify you through a notice on our website.

Policy compliance and enforcement

Examples of non-compliance

Misconduct

Misconduct refers to actions or behaviour by an employee that deviates from the expected standards of conduct outlined in corporate policies or codes of conduct. It typically involves violations of company policies, rules, or guidelines, which may result in minor breaches or disruptions in the workplace. Examples of misconduct include:

1. Failure to properly handle personal data:
    a. Incorrectly categorising data leading to inadequate protection measures.
    b. Improper disposal of documents containing personal data, such as throwing them in a regular bin instead of shredding.
2. Unauthorised access:
    a. Accessing personal data without a legitimate business need or authorisation.
    b. Viewing colleagues' or clients' personal information out of curiosity.
3. Failure to report data breaches:
    a. Delaying the reporting of minor data breaches or security incidents to the relevant authority.
    b. Not following the established procedure for reporting privacy concerns.

Serious misconduct

Serious misconduct refers to actions or behaviour that significantly and detrimentally impact the organisation, its employees, clients, or stakeholders. It involves more severe violations that breach ethical standards, cause harm, or disrupt the workplace environment. Serious misconduct can have legal implications and can result in immediate termination of employment. Examples of serious misconduct include:

1. Intentional data breach:
    a. Deliberately leaking personal information to unauthorised parties.
2. Gross negligence in data protection:
    a. Storing sensitive personal data in unsecured locations or systems.
    b. Ignoring multiple warnings about poor data security practices leading to significant data breaches.
3. Violation of user privacy:
    a. Conducting surveillance on individuals without proper authorisation or legal basis.
    b. Collecting or using personal data for purposes other than those disclosed to and agreed upon by the data subjects.
    c. Malicious disclosure of personal information (“doxxing”)—including publication of private contact details, identity data, or other sensitive information without consent—is strictly prohibited and may result in disciplinary action, contract termination, or referral to law enforcement. the Criminal Code Act 1995 (Cth): s 474.17C & s 474.17D and carries significant penalties.

4. Non-compliance with regulatory requirements:
    a. Failing to implement necessary data protection measures as mandated by laws and regulations.
    b. Ignoring orders from data protection authorities or refusing to cooperate with investigations.

Consequences for non-compliance

While misconduct is considered a breach of company policies, it is typically addressed through disciplinary measures or corrective actions, such as verbal warnings, written warnings, counselling, or performance improvement plans. Due to the severe nature of serious misconduct, immediate and decisive action is often taken, including disciplinary proceedings, investigations, termination, and potential legal consequences.

Identitii recognises the expanded enforcement powers of the OAIC under the Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 and the Privacy and Other Legislation Amendment Act 2024 and is committed to compliance with that framework, including cooperation with investigations, adherence to data security obligations and timely breach notification.

The OAIC is now empowered to take the following regulatory actions:

- Higher civil penalties: the maximum penalty for serious interferences with privacy, introduced by the 2022 amendments, is AUD 50 million, three times the value of any benefit obtained, or 30 per cent of adjusted turnover, whichever is greater, with mid-tier and low-tier penalties for less serious contraventions added by the 2024 amendments.
- Enforceable data security obligations: The OAIC may issue binding directions requiring entities to take corrective action where data security practices are found to be inadequate.
- Expanded breach notification triggers: The Commissioner may investigate and enforce notification obligations even in complex or systemic data breach scenarios, beyond the existing Notifiable Data Breaches scheme.
- Enhanced international cooperation: The OAIC is authorised to share information and coordinate enforcement with international privacy regulators, supporting a consistent approach to global data protection compliance.

Policy monitoring and evaluation

Monitoring and evaluation

Monitoring and evaluating the progress and effectiveness of the policy is crucial to ensure its continuous improvement and alignment with organisational goals. Monitoring and evaluation may be conducted through internal audit, external audit, and manual audits of controls:

1. Internal audit:
    a. Internal audit teams or personnel, independent from the areas being audited, can assess the implementation and compliance of the policy.
    b. Internal audits can include a review of controls, processes, and procedures to determine their effectiveness and identify any gaps or weaknesses.
    c. Internal auditors can conduct regular audits based on an audit plan, which outlines the areas to be audited and the frequency of audits.
    d. The internal audit function can evaluate the organisation's adherence to the policy's requirements, identify areas of non-compliance, and provide recommendations for improvement.
    e. The internal audit team may also assess the effectiveness of processes, risk management practices, and awareness and training programs.
2. External audit:
    a. External audit firms or independent assessors can be engaged to evaluate the organisation's compliance with relevant standards, regulations, or industry best practices.
    b. External audits provide an objective assessment of the organisation's controls and compliance with external requirements.
    c. External auditors may review the organisation's policies, procedures, and controls, and assess their effectiveness in achieving the desired objectives.
    d. External audits can also provide an independent assessment of the organisation's data privacy and protection practices, including compliance with applicable privacy laws and regulations.
3. Manual audits of controls:
    a. Manual audits of controls involve conducting specific assessments of individual controls and processes.
    b. These audits can be performed by designated individuals or teams responsible for managing specific controls, such as access control, financial audits, network security, or data privacy.
    c. Manual audits assess the adequacy and effectiveness of controls, identify any deviations or non-compliance, and recommend corrective actions.
    d. The audits can be conducted through interviews, documentation review, observations, and testing of control effectiveness.
    e. Manual audits help ensure that controls are properly implemented, monitored, and aligned with the policy's requirements.

4. Key considerations:
    a. Monitoring and evaluation efforts should be based on a well-defined audit plan or schedule to ensure regular assessments of different aspects of the policy.
    b. The results of audits, both internal and external, should be documented and shared with relevant stakeholders, such as senior management.
    c. Identified gaps or non-compliance should be addressed through corrective actions and follow-up audits to verify the effectiveness of remedial measures.
    d. Monitoring and evaluation processes should be adaptable to changes in the organisation's environment, emerging threats, and evolving requirements.
    e. It is important to ensure that auditors and assessors possess the necessary expertise and knowledge to effectively evaluate the policy and associated controls.

Review

To ensure the policy remains up-to-date, effective, and aligned with organisational goals, feedback, review, and periodic revisions should be incorporated into the policy management process. Here are mechanisms that can be implemented for these purposes:

1. Feedback mechanisms:
    a. Establish a designated point of contact to receive feedback and suggestions regarding the policy.
    b. Encourage stakeholders to provide feedback through various channels, such as a designated email address, feedback forms, or an anonymous reporting system.
    c. Conduct surveys or focus group discussions to gather insights and perspectives from employees, management, and other stakeholders.
    d. Establish a culture of open communication and encourage stakeholders to proactively raise concerns or provide suggestions related to the policy.
2. Periodic review:
    a. Define a timeline or schedule for conducting periodic reviews of the policy. The frequency may vary depending on the organisation's needs, but typically ranges from annually to biennially.
    b. Form a review committee consisting of representatives from relevant departments to conduct the policy review.
    c. During the review, assess the policy's alignment with emerging threats, changes in regulatory requirements, technological advancements, and lessons learned from incidents or audits.
    d. Solicit feedback from stakeholders during the review process to gather insights on the policy's strengths, weaknesses, and areas for improvement.
    e. Evaluate the policy against industry best practices, standards, and guidelines to ensure its relevance and effectiveness.

3. Revisions and updates:
    a. Based on the feedback and findings from the review process, initiate the necessary revisions and updates to the policy.
    b. Clearly document all changes made to the policy, including the rationale and considerations behind each revision.
    c. Ensure that the revised policy reflects the latest best practices, addresses identified gaps or weaknesses, and incorporates new requirements.
    d. Communicate the revisions to all stakeholders through appropriate channels, such as internal newsletters, email communications, or training sessions.
    e. Ensure that stakeholders have access to the updated policy document and are aware of the changes made.
4. Training and awareness:
    a. Conduct training sessions or awareness programs to educate employees and stakeholders about the revised policy and its implications.
    b. Highlight the changes made, the reasons behind the revisions, and any new responsibilities or requirements resulting from the updated policy.
    c. Reinforce the importance of adhering to the policy and provide guidance on how to comply with the revised guidelines.
    d. Offer refresher training periodically to reinforce key policy concepts and maintain awareness among stakeholders.

Conclusion

This Privacy Policy reflects our commitment to safeguarding personal information and upholding transparency, security and compliance across all data handling activities. It sets out how we collect, use, store, disclose and protect personal information, the rights available to individuals under Australian law and, where applicable, the GDPR, and the steps we take to meet our legal obligations. It also explains how you can exercise your rights, raise concerns, and understand the safeguards we apply in managing personal information throughout its lifecycle.