



Australian Government
Digital Transformation Agency

Privacy Requirements

Trusted Digital Identity Framework
March 2019, version 1.2

Digital Transformation Agency

This work is copyright. Apart from any use as permitted under the Copyright Act 1968 and the rights explicitly granted below, all rights are reserved.

Licence



With the exception of the Commonwealth Coat of Arms and where otherwise noted, this product is provided under a Creative Commons Attribution 4.0 International Licence. (<http://creativecommons.org/licenses/by/4.0/legalcode>)

This licence lets you distribute, remix, tweak and build upon this work, even commercially, as long as they credit the DTA for the original creation. Except where otherwise noted, any reference to, reuse or distribution of part or all of this work must include the following attribution:

Trusted Digital Identity Framework (TDIF™): Privacy Requirements ©
Commonwealth of Australia (Digital Transformation Agency) 2019

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (<http://www.itsanhonour.gov.au>).

Conventions

TDIF documents referenced by this document are denoted in italics. For example, *TDIF: Overview and Glossary* is a reference to the TDIF document titled Overview and Glossary.

The key words “**MUST**”, “**MUST NOT**”, “**SHOULD**”, “**SHOULD NOT**”, and “**MAY**” in this document are to be interpreted as described in the current version of the *TDIF: Overview and Glossary*.

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties accessing this document or have questions or comments regarding this document please email the Director, Digital Identity Policy at identity@dta.gov.au.

Document Management

The TDIF Accreditation Authority has reviewed and endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.01	Mar 2017	JS & DA	Initial version
0.02	May 2017	JS	Updates based on feedback from privacy stakeholders and internal feedback. Updates include: <ul style="list-style-type: none">• Changed headings and restructure of the order of content.• Opt in privacy requirements.• Cross border and contractor disclosure.• Refinement to sections on reporting data breaches, definition of personal information, use and disclosure, consent, Privacy Impact Assessments and government identifiers.• Aligning Governance requirements to announcements about Australian Public Service Privacy Code.
0.03	Jul 2017	SJP	Minor updates to align with other TDIF documents
0.04	Sept 2017	JS	Removed Relying Party. Removal of list of metadata retained by the Exchange. Removal of minimal age limits. Minor updates to support the consultation draft.
0.05	Jan 2018	JS	Updates based on feedback from targeted and public consultation. Merged Privacy Audit document into Privacy Requirements. Aligned requirements to registered Australian Government Agencies Privacy Code.
1.0	Feb 2018		Endorsed for release by the TDIF Accreditation Authority.
1.1	Sept 2018	JS	Addition of limitation on behavioural information Streamlining of consent section so not to duplicate common law requirements Revision of overseas and contractor disclosure section
1.2	Mar 2019	JS	Incorporated feedback from stakeholders and public consultation.

Contents

1 Introduction	1
2 Part one: Privacy requirements.....	2
2.1 General requirements	2
2.2 Privacy governance	3
2.2.1 Roles	3
2.2.2 Policies	4
2.2.3 Internal privacy capability.....	4
2.3 Privacy Impact Assessment.....	5
2.4 Data Breach Response Management.....	6
2.5 Notice of Collection	7
2.6 Collection and use limitation	8
2.6.1 Identity Exchange additional requirements	8
2.7 Limitation on use of behavioural information	9
2.8 Collection and use of biometrics	9
2.9 Consent.....	9
2.9.1 Identity Service Provider additional requirements.....	10
2.10 Cross border and contractor disclosure	10
2.11 Government Identifiers.....	11
2.12 Access, correction and consumer history log	11
2.12.1 Access	11
2.12.2 Correction	11
2.12.3 Consumer history log	12
2.13 Quality of personal information	12
2.13.1 Identity Service Provider additional requirements.....	12
2.14 Handling Privacy Complaints	13
2.15 Destruction and de-identification	13
3 Part two: privacy audit	15
3.1 Purpose and context of the privacy audit.....	15

3.2 Privacy audit process	16
3.3 Type of audit and auditor skills	17
3.4 Privacy audit roles and responsibilities	17
3.4.1 TDIF Accreditation Authority	17
3.4.2 The Applicant	17
3.4.3 Privacy Assessor.....	18
Annex A: Privacy audit template	19

1 Introduction

Agencies and organisations that apply to be accredited under the TDIF undergo a series of rigorous evaluations across all aspects of their identity service operations. The *TDIF: Accreditation Process* requires Applicants to demonstrate their identity service is usable, privacy enhancing and is secure and resilient to cyber threats. The intent of these evaluations is to determine whether the Applicant's identity service meets the TDIF Guiding Principles¹ and whether it is suitable to join the identity federation.

These Privacy Requirements apply whether an Applicant or Accredited Provider is subject to the *Privacy Act 1988* (Cth) (Privacy Act), state or territory privacy legislation or not covered by privacy law. These requirements rely heavily on the Australian Privacy Principles (APPs), other provisions in the Privacy Act and the Australian Government Agencies Privacy Code but are intended to be more specific and provide the highest standard across Australian and state government privacy legislation. The TDIF has incorporated relevant parts of the European Union General Data Protection Regulations (EU GDPR), particularly the consent requirements, but the TDIF does not seek to enforce the EU GDPRs.

The intended audience for this document includes:

- Applicants and Accredited Providers.
- Assessors.
- Relying Parties.
- TDIF Accreditation Authority.

¹ See *TDIF: Overview and Glossary* for further information on the TDIF guiding principles.

2 Part one: Privacy requirements

2.1 General requirements

Identity Exchanges **MUST** operate separately from other identity federation participants and **MUST** establish and maintain its own privacy management arrangements.

The Applicant **MUST** comply with its obligations under the Privacy Act or, where relevant, state or territory privacy legislation and applicable Privacy Codes.

If the Applicant is a small business operator as defined by the Privacy Act, and therefore exempt from the Privacy Act, it **MUST** opt-in to coverage of the APPs as an organisation. Any state or territory government Applicant not covered by state privacy laws providing substantially the same level of protection as the APPs **MUST** comply with APPs for the purpose of achieving TDIF Accreditation².

For the purpose of TDIF accreditation, an Applicant **MUST** protect the greater subset of:

- 'Personal information' as defined by the Privacy Act.
- Information about an individual who has died.
- Where the Identity Service Provider is a state or territory government agency, personal information as defined by a relevant state jurisdiction.
- The data created and retained about the attributes disclosed by an Identity Exchange.

The following privacy requirements apply to all Applicants unless explicitly stated otherwise. There are some requirements on Privacy Assessors under the heading Privacy Audit.

² This will be enforced by the TDIF Accreditation Authority

2.2 Privacy governance

2.2.1 Roles

The Applicant **MUST**:

- Have at least one designated Privacy Officer.
- Ensure Privacy Officers are the primary point of contact for advice on privacy matters.
- Ensure that the following Privacy Officer functions are regularly carried out:
 - Handling of internal and external privacy enquiries, privacy complaints.
 - Requests for access to and correction of personal information made under these Privacy Requirements and privacy legislation.
 - Maintaining a record of the Accredited Providers personal information holdings.
 - Assisting with the preparation of Privacy Impact Assessments (PIAs).
 - Maintaining the Applicant's register of PIAs.
 - Measuring and documenting the Applicant's performance against the privacy management plan and updating privacy policies, at least annually.
- At all times, have a designated Privacy Champion responsible for:
 - Promoting a culture of privacy within the Applicant that values and protects personal information.
 - Providing leadership within the Applicant's organisation on broader strategic privacy issues.
 - Reviewing and approving the Applicant's privacy management plan, and documented reviews of the Applicant's progress against the privacy management plan.
 - Providing regular reports to the Applicant's executive, including about any privacy issues arising from the Applicant's handling of personal information.

An Applicant's designated Privacy Officer **MAY** also be its designated Privacy Champion.

2.2.2 Policies

An Applicant that is an IdP or Exchange **MUST** have a separate privacy policy to that of its other business or agency functions. The Applicant **MUST** publish a clearly expressed and up to date Privacy Policy about its management of personal information which **MUST** contain:

- The kinds of personal information that the entity collects and holds.
- How the entity collects and holds personal information.
- The purposes for which the entity collects, holds, uses and discloses personal information.
- How an individual may access personal information about the individual that is held by the entity and seek the correction of such information.
- How an individual may complain about a breach of the APPs³ and these Privacy Requirements and how the entity will deal with such a complaint.
- Whether the entity is likely to disclose personal information to overseas recipients and if so the countries in which such recipients are likely to be located (if it is practicable to do so).

Privacy Policies **MUST** be regularly (at least annually) reviewed and updated.

The Applicant **MUST**:

- Develop and maintain a privacy management plan which identifies specific, measurable privacy goals and targets; and sets out how an Applicant take steps as are reasonable in the circumstances to implement practices, procedures and systems to implement these Privacy Requirements and other relevant privacy laws.
- Document the Applicant's performance against its privacy management plan at least annually.

2.2.3 Internal privacy capability

The Applicant **MUST**:

³ Or particular jurisdictional Privacy Principle.

- Include appropriate privacy education or training in any staff induction program it provides to staff involved in the Accredited Provider. The privacy education must address the privacy obligations of staff, and policies and procedures relating to privacy, particularly these Privacy Requirements.
- Provide appropriate privacy education or training annually to all staff who have access to personal information in the course of performing their duties as a staff member related to the Applicant's role(s) in the identity federation.
- Regularly review and update its privacy practices, procedures and systems, to ensure their currency and adequacy for the purposes of compliance with these Privacy Requirements and privacy laws.
- Monitor compliance with its privacy practices, procedures and systems regularly.

2.3 Privacy Impact Assessment

As part of the TDIF Accreditation Process, the Applicant:

- **MUST** commission a PIA, by a Privacy Impact Assessor to review the privacy impacts of the Applicant's identity service.
 - A Privacy Impact Assessor is a separate legal entity to the Applicant, not under the Applicant's control and has knowledge and experience in conducting PIAs.
- **MUST** conduct a PIA for all high privacy risk projects related to its identity service.
 - A project may be a high privacy risk project if the Applicant reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.
- **SHOULD** publish the above mentioned PIAs, or a summary version or an edited copy of the PIA, on its website.
- **MUST** respond in writing, at a senior management level, to the recommendations outlined in the PIA including whether the recommendations are accepted, the reasons for any non-acceptance and the timeframe for implementation of the recommendations.
- **MUST** maintain a register of the PIAs it conducts and response.
- **MUST** publish the register, or a version of the register, on its website.

A PIA **SHOULD** be conducted using the *Guide to undertaking privacy impact assessments*⁴.

A PIA **MUST** at a minimum:

- Be conducted by a Privacy Impact Assessor
- Be in writing.
- Be conducted early enough to influence the design of a project or decision.
- Reflect consultation with relevant stakeholders.
- Include a description of the proposed project.
- Map the project's information flows.
- Include an analysis of:
 - Risks of non-compliance with the relevant laws related to privacy.
 - Risks of non-compliance with these Privacy Requirements.
 - The impact of the project on individuals.
 - Whether privacy impacts are necessary or avoidable.
 - Possible mitigation of risks.
- Provide recommendations to the TDIF Accreditation Authority.

2.4 Data Breach Response Management

The Applicant **MUST**:

- Have a documented Data Breach Response Plan (see below).
- For Applicants covered by the *Privacy Act 1988*, report eligible data breaches to individuals and the Information Commissioner as required under the *Privacy Act 1988*⁵ and also report the eligible data breach to the TDIF Accreditation Authority.
- For Applicants not covered by the *Privacy Act 1988*, report eligible data breaches to individuals as described in the *Privacy Act 1988* and also report the eligible data breach to the TDIF Accreditation Authority.

⁴ See *References* for further information on undertaking a PIA.

⁵ See Part IIIC of <https://www.legislation.gov.au/Details/C2019C00025> for the definition of an eligible data breach including exceptions to reporting.

The Data Breach Response Plan⁶ is a tool to help Applicants prepare for a data breach. It **MUST**, at a minimum, include:

- The actions to be taken if a breach is suspected, discovered or reported by a staff member, including a clear communications plan and information about when it is to be escalated to the data breach response team (response team).
- The members of the response team.
- The actions the response team is expected to take.
- Information about how the actions and roles in the plan relates to the Applicant's Incident Response Plan⁷.

2.5 Notice of Collection

The Applicant **MUST**, when it collects personal information of users, take reasonable steps, to notify them of the following:

- Its identity and contact details.
- Any collections from third parties.
- Where relevant, that a collection is required by law and the relevant law.
- The purposes of collection.
- The main consequences for the individual if all or some of the personal information is not collected.
- Any other entity, body or person, or the types of any other entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected.
- The privacy policy contains information about how the individual may access their personal information and seek the correction of such information.
- The Privacy Policy contains information about how the individual may lodge a complaint.
- Whether the entity is likely to disclose the personal information to overseas recipients (and if so, where).

⁶ See *References* for further information on developing a Data Breach Response Plan.

⁷ See *Trust Framework: Protective Security Requirements* for further information on developing an Incident Response Plan.

2.6 Collection and use limitation

The Applicant **MUST** ensure that:

- It only collects personal information that is reasonably necessary for one or more of its functions or activities relating to identity verification.
- It only collects information by lawful and fair means.
- It only collect information from the individual or their representative, unless it is unreasonable or impractical to do so.
- It only collects sensitive information where it is required or authorised by or under an Australian law or court order or is otherwise authorised under APP 3.4.
- The individual has consented to his/her identity attributes being disclosed before he/she verifies to a Relying Party.
- Only discloses the minimum identity attributes required for the Relying Party's transaction (e.g. supply proof of age rather than date of birth if that is all is required).

The Applicant **MUST NOT** use personal information for direct marketing purposes.

The Applicant **MUST** comply with APP 6 for all uses and disclosures as well as complying with more specific Privacy Requirements relating to consent (2.9), direct marketing (2.6), behavioural information (2.7) and biometric information (2.8)).

[For example even if APP 6.2 allows the disclosure of identity attributes to a relying party because it is related to the primary purpose and within reasonable expectations, the Exchange must still obtain consent to pass those attributes due to the more specific requirements in the TDIF Privacy Requirements 2.9.]

2.6.1 Identity Exchange additional requirements

If the Applicant is an Identity Exchange it:

- **MUST** publish in an open and accessible manner an annual 'Transparency Report' that discloses the scale, scope and reasons for access to personal information by enforcement bodies.
- **MUST NOT** retain users' attributes once they are passed from the Identity Service Provider to the Relying Party.

2.7 Limitation on use of behavioural information

An Applicant who collects personal information about an individual's behaviour (such as history and frequency of services received, credential preferences or Identity Service Provider preferences) **MUST NOT** use or disclose that information (for example to sell the data, target a person for compliance activities) except to:

- Verify the person and assist them to obtain the service they are seeking, including assisting relying party to offer the service.
- Detect/identify/investigate/report fraud on the identity system.
- Improve the product or service (ie understanding user pain points and system performance).

2.8 Collection and use of biometrics

An Applicant **MUST** only collect sensitive information as defined in the *Privacy Act 1988* (including biometric information and biometric templates) with the explicit consent of the individual.

A biometric collected to provide evidence of identity (for example matching a person's face to a photo document):

- **MUST NOT** be used for any other purpose.
- **MUST NOT** be disclosed to a third party other than a third party verifying the biometric.
- **MUST** be destroyed once the verification process has concluded.

2.9 Consent

The exchange **MUST** obtain consent from an individual prior to it disclosing attributes to a Relying Party.

Note: Valid consent includes:

- The individual is adequately informed before giving consent.
- Consent is voluntary.
- Consent is current and specific.

The individual has the capacity to understand and communicate their consent.

An individual **MAY** withdraw their consent at any time, and the process to do this **MUST** be easy to use and straightforward.

The Applicant **MUST** inform users of other channels available to verify identity and make clear to the user what the consequences are of declining to provide the required information.

The Applicant **MUST** maintain auditable logs that demonstrate that consent was obtained and is current.

2.9.1 Identity Service Provider additional requirements

If the Applicant is an Identity Service Provider it **MUST**:

- Seek and obtain consent to verify identity attributes at the source such as through the Document Verification Service (DVS) and Face Verification Service (FVS).
- Permanently close a user's account at the request of a user, even if some attributes are retained for some time.

2.10 Cross border and contractor disclosure

Applicants **MUST** comply with APP 8 - cross border disclosure of personal information⁸.

In addition, before an Applicant discloses personal information to an overseas recipient as part of running the Applicant (for example an overseas cloud host), the Applicant **MUST** take such steps that are reasonable to ensure the recipient only uses the information for purposes related to identity verification.

When the Applicant contracts the operation of a part of its business covered by the TDIF, the Applicant **MUST** provide evidence to the TDIF Accreditation Authority that it has appropriate contractual and practical measures to ensure the contractor is complying with these Privacy Requirements.

⁸ See Australian Privacy Principle 8 at www.legislation.gov.au/Details/C2017C00283

See the *TDIF: Protective Security Requirements* for more information on security and contract management.

2.11 Government Identifiers

Applicants that are organisations as defined by the Privacy Act **MUST** comply with their obligations under APP 9 which relate to the adoption, use and disclosure of government related identifiers.

An Applicant **MUST NOT** create a new government identifier that is used across the identity federation (i.e. an identifier that is sent to more than one Relying Party or Identity Service Provider).

2.12 Access, correction and consumer history log

2.12.1 Access

The Applicant **MUST**:

- Where it holds personal information about an individual, on request by the individual, give the individual access to the information.
 - Unless an exception is available under APP 12 (APP 12.2 for Commonwealth agencies and APP 12.3 for other Applicants).
- Respond to the request for access to personal information within 30 days after the request is made.
- Give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.
- Provide access for free.
- Where access is refused, take steps to meet the needs of the individual and provide a written notice as set out in APP 12.

2.12.2 Correction

The Applicant **MUST**:

- Allow individuals to correct their personal information as set out in APP 13.
- Provide individuals with a simple means to review and update their personal information on an ongoing basis.

2.12.3 Consumer history log

If the Applicant is an Identity Exchange it **MUST** provide individuals with access to the metadata on transactions it logs (i.e. that has not been deleted under its destruction policy) in one place.

The log **SHOULD** include the services the individual accessed, the time of access and the attributes passed to the service.

Note: an Identity Exchange will not be able to directly identify an individual and therefore the individual will need to access its metadata by logging on through an Identity Service Provider.

2.13 Quality of personal information

The Applicant **MUST**:

- Take reasonable steps to ensure that the personal information it collects is, having regard to the purpose of the use or disclosure is accurate, up-to-date, complete, relevant and not misleading.
- Take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure is accurate, up-to-date, complete, relevant and not misleading.

2.13.1 Identity Service Provider additional requirements

If the Applicant is an Identity Service Provider it **MUST**:

- Implement internal practices, procedures and systems to audit, monitor, identify and correct poor quality personal information (including training staff in these practices, procedures and systems).

- Ensure updated or new personal information is promptly added to relevant existing records.
- Provide individuals with a simple means to review and update their personal information on an ongoing basis.

2.14 Handling Privacy Complaints⁹

The Applicant **MUST** provide a complaints service which:

- Is accessible, including prominent contact information about the service.
- Is fair, including a process that is impartial, confidential and transparent.
- Has a process which is timely, clear and can provide a remedy.
- Has skilled and professional people who have knowledge of privacy laws and these Privacy Requirements and the complaint service process.
- Is integrated with other complaint handling bodies, (e.g. other participants of the identity federation) so it can assist the user and refer complaints.
- Analyses complaint information, including complaint processes, and feeds conclusions into privacy risk planning and improving documentation and processes.
- Publishes de-identified information and analysis about complaints.

The Applicant **MUST** participate in a service that enables agreed de-identified data on complaints to be shared across participants in the identity federation to ensure participants learn from complaints.

2.15 Destruction and de-identification

The Applicant **MUST** ensure that:

- It takes reasonable steps to destroy or de-identify personal information once it is no longer needed for identity verification and related administrative purposes, unless retention is required under law.
- It has a written management policy that specifies:

⁹ See *References* for further information on handling privacy complaints in organisations.

- Whether stored personal information needs to be retained under law or a court/tribunal order.
- Data retention timeframes.
- De-identification policies and practices (including mitigation of the risk of re-identification).
- Data destruction policies and practices.
- All staff are informed of document destruction and de-identification procedures.
- Where required, personal information contained in hard copy records is destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding.
- Hardware containing personal information (including back-ups) in electronic form is 'sanitised' in accordance with Australian Signals Directorate requirements to completely remove the stored personal information.
- Where personal information is stored on a third-party's hardware (e.g. cloud storage) procedures are in place to verify that instructions to irretrievably destroy/de-identify the personal information have been complied with.

3 Part two: privacy audit

3.1 Purpose and context of the privacy audit

This section outlines the requirements and provides some guidance for Applicants and Privacy Assessors when conducting the privacy audit as part of the TDIF Accreditation Process.

The privacy audit is required after the Applicant has performed a PIA and submitted evidence to the TDIF Accreditation Authority to address these Privacy Requirements.

The aim of the privacy audit is to:

- Determine whether the Applicant can demonstrate it has complied with these Privacy Requirements.
- Determine whether the Applicant has addressed all recommendations arising from the PIA.
- Document the results of the privacy audit in a report to the TDIF Accreditation Authority.

The following activities have occurred by the time the privacy audit is undertaken:

- The Applicant has provided the TDIF Accreditation Authority with a plan demonstrating how they will meet these Privacy Requirements.
- The Applicant has provided the TDIF Accreditation Authority with privacy documentation including a Privacy Management Plan and Data Breach Plan. The full list of privacy documentation is outlined above in the 'Privacy Requirements' section of this document.
- An independent body has conducted a PIA on the Applicant.
- The Applicant has provided the TDIF Accreditation Authority with a report which outlines how and by when they will address the recommendations outlined in the PIA.
- As part of the TDIF Accreditation Process the Applicant has submitted protective security, risk management and fraud control documentation to the TDIF Accreditation Authority. This provides additional context to the privacy audit.

3.2 Privacy audit process

The Privacy Assessor **MUST** carry out the following steps as part of the privacy audit:

- Evaluate assessments or comments already made by the TDIF Accreditation Authority.
- Evaluate all relevant evidence provided by the Applicant to the TDIF Accreditation Authority. This includes any responses to questions which may have been asked.
- Once the documentation has been reviewed, define the scope, objectives and criteria of the privacy audit as part of an audit plan.
- Conduct the privacy audit. At a minimum this **MUST** include:
 - Documentation reviews.
 - Conduct a site visit.
 - Interview key privacy and operations personnel.
- The Privacy Assessor **MUST** retain evidence to support its findings. The Privacy Assessor will only need to provide evidence indicated in the privacy audit tool below to the TDIF Accreditation Authority as part of its report.
- Provide the Applicant with reasonable opportunity to provide feedback on its evidence and findings.
- Provide the Applicant with reasonable opportunity to respond to the report's findings, including the actions and timeframes in which remediation actions will occur. This is required if non-compliance issues are identified.
- Provide a report of findings (see *Annex A: privacy audit template* below) to the Authority. The report **MUST** at a minimum:
 - Summarise the activities performed during the privacy audit.
 - Advising whether or not the Applicant has complied with these Privacy Requirements, including any requirements that could not be adequately assessed due to access or timing issues.
 - Recommends remediation actions to address any areas of non-compliance.
 - Include the Applicant's response to the privacy audit findings and recommendations.

3.3 Type of audit and auditor skills

The privacy audit is to determine whether the Applicant is compliant with these Privacy Requirements and has addressed the PIA recommendations. The Privacy Assessor **MUST NOT** take a ‘tick box’ approach to the requirements.

The privacy audit **MUST** be undertaken by an Privacy Assessor who is independent from the development team. Privacy Assessors can either be internal staff or third parties.

The Privacy Assessor **MUST** have relevant and adequate experience and training to carry out the privacy audit.

3.4 Privacy audit roles and responsibilities

3.4.1 TDIF Accreditation Authority

The TDIF Accreditation Authority is responsible for:

- Ensuring that the accreditation process is conducted with due care and in accordance with the published TDIF documents.
- Reviewing, within agreed timeframes, all relevant Applicant documentation to ensure conformance to the published TDIF documents.
- Providing relevant documentation, it holds on an Applicant to the auditor.
- Considering all reports and recommendations from Privacy Assessors.
- Notify the Applicant of any non-compliance issues, required mitigation actions and timeframes for the mitigations.
- All decisions in relation to the suitability of an Applicant to be accredited.

3.4.2 The Applicant

The Applicant is responsible for:

- Obtaining the services of an auditor.
- Preparing and providing all information requested by the auditor.
- Supporting the auditor as required during the privacy audit.

- Responding to the auditor and TDIF Accreditation Authority regarding proposed remediation activities and timeframes.
- Remediating all identified non-compliance issues to the satisfaction of the TDIF Accreditation Authority.

3.4.3 Privacy Assessor

The Privacy Assessor is responsible for:

- Assessing the Applicant's compliance against these Privacy Requirements.
- Documenting their findings, which:
 - Summarise the activities performed during the evaluation.
 - Suggest remediation actions to address areas of non-compliance or unmitigated risk.
 - Recommend whether or not the Applicant has satisfied these Privacy Requirements.
- Providing their findings to the TDIF Accreditation Authority.

Annex A: Privacy audit template

Trusted Digital Identity Framework – Privacy audit		
Date of audit:		
Date of audit report:		
Name of auditor:		
Summary of activities performed during the privacy audit:		
<ul style="list-style-type: none"> 1 2 		
Remediation actions and other notes <ul style="list-style-type: none"> Add remediation actions to each Privacy Requirement where there is a non-compliance Add notes the Trust Framework Accreditation Authority should be made aware of 		
Privacy Requirement PIA Recommendation	compliance non-compliance	Required attachment Accreditation Authority notes
Privacy Governance		
Privacy Impact Assessment		
Data Breach Response Management		
Notice of Collection		
Collection and use limitation		
Biometric collection		
Behavioural information		
Consent		
Cross border and contractor disclosure		
Government Identifiers		
Access, correction and dashboard		
Quality of personal information		
Handling of privacy complaints		
Destruction and de- identification		
PIA recommendations		