Australian Government
Digital Transformation Agency

04 - Functional Requirements

Trusted Digital Identity Framework Release 4
January 2021, version 1.1

PUBLISHED VERSION

dta

Digital Transformation Agency (DTA)

Licence

Use of the Coat of Arms

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

Conventions

References to *TDIF* documents, abbreviations and key terms (including the words *MUST*, *MUST NOT*, and *MAY)* are denoted in italics are to be interpreted as described in the current published version of the *TDIF: 01 – Glossary of Abbreviations and Terms.*

TDIF requirements and references to *Applicants* are to be read as also meaning *Accredited Participants*, and vice versa. The scope of *TDIF* requirements are to be read as applying to the identity system under *Accreditation* and not to the organisation's broader operating environment.

Contact us

The *DTA* is committed to providing web accessible content wherever possible. This document has undergone an accessibility check however, if you are having difficulties with accessing the document, or have questions or comments regarding the document please email the Director, Digital Identity Policy at identity@dta.gov.au.

Document management

The *DTA* has reviewed and endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.1	Aug 2019	SJP	Initial version
0.2	Oct 2019	SJP	Updated to incorporate feedback provided by stakeholders during the first round of collaboration on TDIF Release 4
0.3	Dec 2019	JS, SJP	Updated to incorporate feedback provided by stakeholders during the second round of collaboration on TDIF Release 4
0.4	Mar 2020	JS, SJP	Updated to incorporate feedback provided during the public consultation round on TDIF Release 4
1.0	May 2020		Published version
1.1	January 2021	JK	CRID0005 – Emergency Change to ASSESS-07-03-01 (minor typo)

Document review

The next scheduled review of this document will occur by July 2022. Any changes made to the document prior to this date will be recorded in a *TDIF* change management document and published to the *DTA* website.

Contents

1 Introduction

This document sets out the *TDIF functional requirements* to be met by *Applicants* in order to achieve *TDIF* accreditation.

These *TDIF functional requirements* do not replace, remove or diminish existing obligations imposed on government agency or organisations through other policies, legislation or regulations, or by any other means. These *TDIF functional requirements* supplement existing obligations and apply specifically to *identity* services that undergo the *TDIF Accreditation Process*.

The intended audience for this document includes:

- *Accredited Participants.*
- *Applicants.*
- *Assessors.*
- *Relying Parties.*

2 Fraud Control Requirements

Several requirements listed in this section incorporate *fraud* control advice, guidance, policies and publications developed by the Australian Government. This includes the *Commonwealth Fraud Control Framework* (*CFCF*)[1] and *Australian Government Investigation Standards* (*AGIS*)[2] developed by the *Australian Government Attorney General's Department*. These requirements ensure *Applicants* establish a minimum *fraud* control baseline for their *identi*ty service.

Applicants that undergo the *TDIF Accreditation Process* should note the following:

- Refences to 'agencies', 'accountable authority', 'Commonwealth entities', 'entities', 'officials', 'Australian Government' in the CFCF or AGIS are to be interpreted as being applicable to the *Applicant*.
- The scope of CFCF controls are limited to the identity service being accredited and not to the *Applicant's* wider operating environment.

To the extent of conflict between:

- Any requirement in these *TDIF* requirements and the current edition of the *CFCF*, then the *CFCF* takes precedence.
- Any requirement in these *TDIF* requirements and the current edition of the *AGIS*, then the *AGIS* takes precedence.
- The *AGIS* and law, then the legislative requirement will prevail.

2.1 Accountable Authority

TDIF Req: FRAUD-02-01-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* <u>*MUST*</u> appoint a senior executive as the designated *Accountable Authority* for managing *fraud* risks within its organisation.

1 A copy of the *CFCF* is available at https://www.ag.gov.au/Integrity/counter-fraud/fraud-australia/Documents/CommonwealthFraudControlFramework2017.PDF

2 A copy of the *AGIS* is available at https://www.ag.gov.au/Integrity/counter-fraud/fraud-australia/Documents/AGIS%202011.pdf

TDIF Req: FRAUD-02-01-02; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Accountable Authority* *MUST*:

a) Determine the *Applicant's* tolerance for *fraud* risks.
b) Manage the *Applicant's fraud* risks.
c) Demonstrate how its *fraud* controls are applied to its identity system.
d) Take all reasonable measures to prevent, detect and deal with *fraud* relating to its identity system.
e) Consider the implications their risk management decisions have for other organisations and share information on risks where appropriate.

TDIF Req: FRAUD-02-01-03; **Updated**: Mar-20; **Applicability**: A, C, I, X

Where exceptional circumstances prevent or affect the *Applicant's* capability to implement a *TDIF* requirement, the *Accountable Authority*:

a) *MUST* record the decision to vary its *fraud* control arrangements and advise the *DTA* of remedial action taken to reduce the risk to their business operations. These decisions will be requested by the *DTA* during *Annual Assessments*.
b) *MAY* vary application, for a limited period, consistent with the *Applicant's* risk tolerance.

2.2 Fraud control plan

TDIF Req: FRAUD-02-02-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* have in place a *Fraud Control Plan* approved by the *Accountable Authority* to manage the *Applicant's fraud* risks.

TDIF Req: FRAUD-02-02-01a; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Fraud Control Plan* *MUST* detail the:

a) *Fraud* control goals and strategic objectives of the *Applicant*, including how the management of *fraud* risks intersects with and supports broader business objectives and priorities.
b) *Applicant's* strategies to implement *fraud* risk management and maintain a positive risk culture.

c) *Applicant's* tolerance to *fraud* risks.
d) *Fraud* threats, risks and vulnerabilities that impact the protection of the *Applicant's* people, information (including *ICT*) and assets.
e) Maturity of the *Applicant's* capability to manage *fraud* risks.
f) Treatment strategies and controls put in place to manage *fraud* threats, risks and vulnerabilities.
g) Strategies to ensure the *Applicant* meets its training and awareness needs
h) Procedures and mechanisms for *fraud* incident management, *fraud* investigations and reporting *fraud* incidents.
i) An outline of key roles and responsibilities for *fraud* control within the *Applicant's* organisation.

Where a single *fraud control plan* is not practicable due to the *Applicant's* side or complexity of business, the *Accountable Authority* may approve a strategic-level overarching *fraud control plan* that addresses the requirements listed above.

TDIF Req: FRAUD-02-02-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Fraud Control Plan* (and supporting *Fraud Control Plans*) *MUST* be reviewed annually by the *Applicant's Accountable Authority* and when there is a change in the structure, functions or activities of the *Applicant* which impact the operation of the fraud control components of their identity system.

TDIF Req: FRAUD-02-02-02a; **Updated**: Mar-20; **Applicability**: A, C, I, X
This review *MUST*:

a) Determine the adequacy of existing fraud control measures and mitigation controls.
b) Respond to and manage shifts in the *Applicant's* risk, threat and operating environment.

2.3 Fraud prevention, awareness and training

TDIF Req: FRAUD-02-03-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant MUST* provide all *Personnel* with *fraud* awareness training at engagement and annually thereafter. A copy of these training materials will be

requested by the DTA as part of initial accreditation and annually thereafter as part of the *Annual Assessment*.

TDIF Req: FRAUD-02-03-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* demonstrate to the *DTA* how it considers the risk of *fraud* when planning and conducting activities associated with the operation of its identity system.

TDIF Req: FRAUD-02-03-03; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* maintain appropriately documented instructions and procedures to assist personnel prevent, detect, report and deal with fraud.

TDIF Req: FRAUD-02-03-04; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* ensure *Personnel* primarily engaged in *fraud* control activities possess or attain relevant qualifications or training.

TDIF Req: FRAUD-02-03-05; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* conduct background checks on individuals prior to their commencement of employment with the *Applicant* and on *Personnel* with access to Personal information.

TDIF Req: FRAUD-02-03-06; **Updated**: Mar-20; **Applicability**: A, C, I
The *Applicant* *MUST* provide fraud-control advice to *Users* on how to safeguard their *Digital Identity* and *Attributes*.

TDIF Req: FRAUD-02-03-07; **Updated**: Mar-20; **Applicability**: A, C, I
Where identity-related scams are detected, the *Applicant* *MUST* provide advice to *Individuals* on how to avoid being scammed.

2.4 Fraud monitoring and detection

TDIF Req: FRAUD-02-04-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* implement a mechanism for detecting incidents of *fraud* or suspected *fraud*, including a process for *Personnel* and users to report suspected *fraud* confidentially.

TDIF Req: FRAUD-02-04-02; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* implement a *fraud* control mechanism to flag incidents of *fraud* or suspected fraud.

TDIF Req: FRAUD-02-04-02a; **Updated**: Mar-20; **Applicability**: A, C, I

The *Applicant* *MUST* compare all new registrations and updates to existing records against the *fraud* control mechanism used to flag incidents of *fraud* or suspected fraud.

TDIF Req: FRAUD-02-04-02b; **Updated**: Mar-20; **Applicability**: A, C, I

The *Applicant* *MUST NOT* allow a new registration or update to be completed if the *fraud* control mechanism indicates the registration or update is fraudulent or suspected fraud.

2.5 Incident management, investigations and reporting

TDIF Req: FRAUD-02-05-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* implement a mechanism for investigating or otherwise dealing with incidents of *fraud* or suspected fraud.

TDIF Req: FRAUD-02-05-02; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* maintain documented procedures setting out criteria for making decisions at critical stages in managing a suspected *fraud* incident.

TDIF Req: FRAUD-02-05-03; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* have in place investigation and referral processes and procedures that are consistent with the *AGIS*.

TDIF Req: FRAUD-02-05-04; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* document decisions to use civil, administrative or disciplinary procedures, or to take no further action in response to a suspected *fraud* incident.

TDIF Req: FRAUD-02-05-05; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* take responsibility for investigating instances of *fraud* or suspected *fraud* against it, including investigating disciplinary matters, unless the matter is referred to and accepted by the *Australian Federal Police* (*AFP*) or another law enforcement agency.

TDIF Req: FRAUD-02-05-06; **Updated**: Mar-20; **Applicability**: A, C, I, X
Where a law enforcement agency declines a referral, the *Applicant* *MUST* resolve the matter in accordance with relevant internal and external requirements.

TDIF Req: FRAUD-02-05-07; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* refer all instances of potential or serious or complex *fraud* offences to the *AFP* in accordance with the *AGIS* and *AFP* referral process, except in the following circumstances:

a) Where legislation sets out specific alternative arrangements.
b) Where the *Applicant*:
    i. Has the capacity and the appropriate skills and resources needed to investigate potential criminal matters.
    ii. Meets the requirements of the *AGIS* for gathering evidence and the *Commonwealth Director of Public Prosecutions* (*CDPP*) in preparing briefs of evidence.

TDIF Req: FRAUD-02-05-08; **Updated**: Mar-20; **Applicability**: A, C, I, X
Fraud investigations *MUST* be carried out by appropriately qualified *Personnel* as set out in the *AGIS*. If external investigators are engaged, they must as a minimum meet the investigations competency requirements set out in the *AGIS*.

TDIF Req: FRAUD-02-05-09; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* take all reasonable measures to recover financial losses caused by illegal activity through proceeds of crime and civil recovery processes or administrative remedies.

TDIF Req: FRAUD-02-05-10; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* develop and use procedures to report incidents of *fraud* or suspected *fraud* to the *Oversight Authority* and *DTA*.

TDIF Req: FRAUD-02-05-10a; **Updated**: Mar-20; **Applicability**: A, C, I, X
As soon as they become aware the *Applicant* *MUST* report incidents of *fraud* or suspected *fraud* to the *Oversight Authority* and *DTA*.

TDIF Req: FRAUD-02-05-10b; **Updated**: Mar-20; **Applicability**: A, C, I, X

a) The *Applicant* *MUST* include the following information when reporting on incidents of *fraud* or suspected fraud: Date and time of the *fraud* incident.

b) Quantity of *fraud* incidents and their level of severity.
c) Time taken to respond to the *fraud* incident.
d) Measures taken in response to the *fraud* incident.
e) Type(s) of fraud.
f) If applicable, the *Identity Proofing Level* and *Credential Level* of the impacted identity record(s).
g) Any other supporting information (e.g. attack vectors used by the fraudster).

Depending on the nature of the *fraud* incident and legal advice obtained, the *Oversight Authority* or *DTA* may advise impacted stakeholders of the outcome of a *fraud* investigation.

2.6 Support for victims of identity fraud

TDIF Req: FRAUD-02-06-01; **Updated**: Mar-20; **Applicability**: A, C, I
The *Applicant* *MUST* implement a process which allows *Users* to notify it when they suspect or become aware of fraudulent use of their *Attributes*, *Digital Identity* or *Credentials*.

TDIF Req: FRAUD-02-06-02; **Updated**: Mar-20; **Applicability**: A, C, I
The *Applicant* *MUST* provide (either directly or through a third party) support services to *Users* whose *Attributes*, *Digital Identity* or *Credential* have been compromised.

TDIF Req: FRAUD-02-06-03; **Updated**: Mar-20; **Applicability**: A, C, I

The *Applicant* *MUST* have in place processes such as appropriate identification of an *Individual* whose *Attributes*, *Digital Identity* or *Credential* has been compromised and appropriate technologies to enable the applicant to flag the *Attributes*, *Digital Identity* or *Credential* as compromised.

TDIF Req: FRAUD-02-06-04; **Updated**: Mar-20; **Applicability**: A, C, I
The Applicant *MUST* prevent the fraudulent use of a *User's Attributes*, *Digital Identity* or *Credentials* (including continued fraudulent activity) once the *Applicant* suspects or it becomes aware of the fraudulent use.

TDIF Req: FRAUD-02-06-05; **Updated**: Mar-20; **Applicability**: A, C, I

When an *Individual* is identified by the *Applicant* as a victim of fraud, or the *Individual* self-identifies, their existing record *MUST* be reproofed to the highest *Identity Proofing Level* which they have previously met.

3 Privacy Requirements

3.1 General privacy requirements

TDIF Req: PRIV-03-01-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The Applicant *MUST* comply with its obligations under the *Privacy Act*, including the *Australian Privacy Principles* (*APPs*), and *Australian Government Agencies Privacy Code* or, where relevant, state or territory privacy legislation.

TDIF Req: PRIV-03-01-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
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.

TDIF Req: PRIV-03-01-03; **Updated**: Mar-20; **Applicability**: A, C, I, X
Any state or territory government *Applicant* not covered by state privacy laws or not prescribed under s6F of the *Privacy Act 1988* *MUST* comply with *APPs* for the purpose of achieving and maintaining *TDIF* accreditation.

3.2 Privacy governance

3.2.1 Privacy roles

TDIF Req: PRIV-03-02-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* have at least one designated *Privacy Officer* who is the primary point of contact for advice on privacy matters.

TDIF Req: PRIV-03-02-01a; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* demonstrate how the following *Privacy Officer* functions are carried out:

a) Handling of internal and external privacy enquiries and complaints.
b) Handles requests for access to and correction of *Personal information*.
c) Maintaining a record of *Personal information* holdings.
d) Assisting with the preparation of *Privacy Impact Assessments* (*PIAs*).

e) Maintaining a register of *PIAs*.
f) Measuring and documenting performance against the *Privacy Management Plan* and reviewing and, where relevant updating, the *Privacy Policy* at least annually relevant to the *TDIF*.

TDIF Req: PRIV-03-02-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* have at least one designated *Privacy Champion*.

TDIF Req: PRIV-03-02-02a; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* demonstrate how its *Privacy Champion* promotes a culture of privacy that values and protects *Personal information*.

TDIF Req: PRIV-03-02-02b; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* demonstrate how its *Privacy Champion* approves its *Privacy Management Plan*, and reviews of the Applicant's progress against the *Privacy Management Plan*.

3.2.2 Privacy Policy

TDIF Req: PRIV-03-02-03; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* publish a clearly expressed and up to date *Privacy Policy* about the management of *Personal information* by the entity.

TDIF Req: PRIV-03-02-03a; **Updated**: Mar-20; **Applicability**: I, X
The *Applicant* *MUST* have a separate *Privacy Policy* in relation to its identity system to that of its other business, organisation functions or *Accredited Roles*.

TDIF Req: PRIV-03-02-03b; **Updated**: Mar-20; **Applicability**: I, X
The *Applicant MUST* maintain separate *Privacy Policies* for their *Identity Service Provider* and *Identity Exchange* if they are accredited in both roles (i.e. a *Privacy Policy* for their *Identity Service Provider* and a separate *Privacy Policy* for their *Identity Exchange*).

TDIF Req: PRIV-03-02-04; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant's Privacy Policy* *MUST* include information on:

a) The kinds of *Personal information* that the entity collects and holds.
b) How the entity collects and holds *Personal information.*

c) The purposes for which the *Applicant* collects, holds, uses and discloses *Personal information*.
d) How an *Individual* can access *Personal information* about themselves that is held by the *Applicant* and how to seek the correction of such information.
e) How an *Individual* can complain about a breach of the *APPs* (or a particular jurisdiction privacy principle) and how the *Applicant* will deal with such a complaint.
f) Whether the *Applicant* 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).

TDIF Req: PRIV-03-02-05; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant's Accountable Authority* MUST review the *Privacy Policy* which covers its identity system at least annually.

3.2.3 Privacy Management Plan

TDIF Req: PRIV-03-02-06; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant's Accountable Authority* MUST develop and maintain a *Privacy Management Plan* that identifies measurable privacy goals and targets for its identity system and the practices, procedures and systems that will be implemented to achieve these targets and goals.

TDIF Req: PRIV-03-02-07; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant's Accountable Authority* MUST measure and document its performance against the *Privacy Management Plan* relevant to TDIF at least annually.

3.2.4 Privacy awareness training

TDIF Req: PRIV-03-02-08; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* MUST on an annual basis, provide privacy awareness training which incorporates these *TDIF* privacy requirements, to all *Personnel* that access the *Applicant's* identity system. A copy of these training materials will be requested by the

DTA as part of initial accreditation and annually thereafter as part of the *Annual Assessment*.

TDIF Req: PRIV-03-02-09; **Updated**: Mar-20; **Applicability**: A, C, I, X

The privacy awareness training provided by the *Applicant*, *MUST* cover the *Applicant's Privacy Policy* and include the TDIF privacy requirements.

3.3 Privacy Impact Assessment

Further information on the *PIA* is outlined in Section 7.1.

TDIF Req: PRIV-03-03-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* maintain a register of the *PIAs* it conducts.

TDIF Req: PRIV-03-03-01a; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* publish the register, or a version of the register, on its website.

3.4 Data Breach Response Management

TDIF Req: PRIV-03-04-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

An *Applicant*, covered by the *Privacy Act, MUST* report eligible data breaches to affected individuals and the *Information Commissioner* as required under the *Privacy Act*[3] and also report the eligible data breach to the *Oversight Authority* and *DTA*.

TDIF Req: PRIV-03-04-01a; **Updated**: Mar-20; **Applicability**: A, C, I, X

An *Applicant*, not covered by the *Privacy Act, MUST* report eligible data breaches as defined in the *Privacy Act 1988* to affected individuals and the *Oversight Authority* and *DTA*.

TDIF Req: PRIV-03-04-02; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* develop and maintain a *Data Breach Response Plan* that includes a description of the actions to be taken if a breach is suspected, discovered, or reported by *Personnel* or external party, including a clear communication plan and

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

information about when it is to be escalated to the data breach response team or third party.

TDIF Req: PRIV-03-04-03; **Updated**: Mar-20; **Applicability**: A, C, I, X

The Data *Breach Response Plan* *MUST*:

a) List the roles or members of the response team.
b) List the actions the response team is expected to take.
c) Describe how the actions and roles in the plan align to the *Applicant's Incident Response Plan*[4].

3.5 Notification of Collection

TDIF Req: PRIV-03-05-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* notify or make people aware as required by *APP* 5.

3.6 Collection and use limitation

TDIF Req: PRIV-03-06-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* only collect *Personal information* that it is permitted to collect under law and that is reasonably necessary for one or more of its functions or activities directly relating to identity verification.

TDIF Req: PRIV-03-06-02; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* only collect *Personal information* by lawful and fair means.

TDIF Req: PRIV-03-06-03; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* only collect *Personal information* from the *Individual* or their representative, unless it is unreasonable or impractical to do so.

TDIF Req: PRIV-03-06-04; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST NOT* use *Personal information* for direct marketing purposes as defined in APP 7.

TDIF Req: PRIV-03-06-05; **Updated**: Mar-20; **Applicability**: X

[4] See *Section 4* for further information on the *Incident Response Plan*.

The *Applicant* *MUST* publish in an open and accessible manner an *Annual Transparency Report* that discloses the scale, scope and reasons for access to *Personal information* (including metadata) by an enforcement body, as defined in the *Privacy Act*.

TDIF Req: PRIV-03-06-06; **Updated**: Mar-20; **Applicability**: X
The *Applicant* *MUST NOT* retain *Users' Attributes* once they are passed from an *Identity Service Provider* to a *Relying Party* with the exception of securely storing the attributes for the duration of an authenticated session.

3.7 Limitation on use of behavioural information

TDIF Req: PRIV-03-07-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* only collect, use and disclose information about an *Individual's* behaviour on the *Australian Government's identity federation* to:

a) Verify the *Identity* of an *Individual* and assist them to receive a digital service from a relying party.
b) To support identity *fraud* management functions.
c) To improve the performance or usability of the *Applicant's* identity system.
d) To de-identify the data to create aggregate data.

3.8 Collection and disclosure of biometrics

TDIF Req: PRIV-03-08-01; **Updated**: Mar-20; **Applicability**: I
The *Applicant* *MUST* only collect *Sensitive information* (including *Biometric information*) as outlined in *APP* 3.3 and 3.4.

TDIF Req: PRIV-03-08-02; **Updated**: Mar-20; **Applicability**: I
Biometric information collected to for the purpose of proofing an *Individual's Identity* *MUST* be destroyed once the *Biometric information* has been used to verify that identity (for example it has been matched against a source photograph), unless:

- The *Individual* chooses to retain the *Biometric information* stored or controlled by the *Individual* on their device, or

- The *Biometric information* is collected or was collected to create a government *Identity document* (for example where a *Road Traffic and Transport Authority* is a, *Identity document issuer* and an *Identity Service Provider*)

TDIF Req: PRIV-03-08-03; **Updated**: Mar-20; **Applicability**: I
Biometric information collected to prove an *Individual's Identity* *MUST NOT* be used and disclosed for purposes other than those listed in **TDIF Req:** PRIV-03-08-02.

3.9 Consent

TDIF Req: PRIV-03-09-01; **Updated**: Mar-20; **Applicability**: A, C, I[5], X
The *Applicant* *MUST* obtain *Express Consent* from an *Individual* prior to disclosing the individual's *Attributes* to a *Relying Party* or any third party.

TDIF Req: PRIV-03-09-01a; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* only disclose the *Individual's Attributes* required for the *Relying Party's* transaction with that *Individual's Consent*.

TDIF Req: PRIV-03-09-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* allow an *Individual* to withdraw their *Consent*.

TDIF Req: PRIV-03-09-02a; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* demonstrate how this *Consent* withdrawal process is straightforward and easy to use.

TDIF Req: PRIV-03-09-02b; **Updated**: Mar-20; **Applicability**: A, C, I, X
An Individual *MUST* be made aware of the implications of providing or withdrawing their *Consent*.

TDIF Req: PRIV-03-09-03; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* maintain auditable logs that demonstrate that *Consent* was obtained and is current.

TDIF Req: PRIV-03-09-03a; **Updated**: Mar-20; **Applicability**: A, C, I, X
The auditable logs *MUST NOT* contain *Biometric information*.

5 If the *Identity Service Provider* connects directly with a *Relying Party*, it is required to obtain express consent prior to the disclosure. If the connection to the *Relying Party* is brokered by an *Identity Exchange*, express consent may be obtained by the *Identity Exchange* on behalf of the *Identity Service Provider*.

TDIF Req: PRIV-03-09-04; **Updated**: Mar-20; **Applicability**: A, I
The *Applicant* *MUST* inform *Individuals* of other channels available to verify *Identity* and make clear to the *User* what the consequences are of declining to provide *Consent* or the required information.

TDIF Req: PRIV-03-09-05; **Updated**: Mar-20; **Applicability**: A, I
The *Applicant* *MUST* obtain *Consent* to verify *Identity Attributes* against an *Authoritative Source*. For example, through an *Identity Matching Service*.

3.10 Cross border and contractor disclosure of Personal information

TDIF Req: PRIV-03-10-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* demonstrate how it complies with *APP* 8 - cross border disclosure of *Personal information*.

TDIF Req: PRIV-03-10-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* take reasonable steps to ensure an overseas recipient of *Personal information* used by the Applicant to provide its identity system only uses the *Personal information* disclosed to it for purposes directly related to identity verification.

TDIF Req: PRIV-03-10-02a; **Updated**: Mar-20; **Applicability**: A, C, I, X
If it discloses *Personal information* to an overseas recipient that is not the individual, the *Applicant* *MUST* demonstrate to the Oversight's reasonable satisfaction it has appropriate contractual and practical measures to ensure the overseas recipient complies with these *TDIF* privacy requirements.

3.11 Government Identifiers

TDIF Req: PRIV-03-11-01; **Updated**: Mar-20; **Applicability**: X
The *Applicant* *MUST NOT* create a new government identifier for use across the identity federation (i.e. an identifier that is sent to more than one *Relying Party* or *Identity Service Provider*).

3.12 Access, correction and individual history log

3.12.1 Access

TDIF Req: PRIV-03-12-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* on request by an *Individual*, give that *Individual* access to the *Personal information* it holds about the *Individual*, unless an exception is available under *APP* 12 (*APP* 12.2 for Commonwealth agencies and *APP* 12.3 for other Applicants).

TDIF Req: PRIV-03-12-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* respond to a request for access to *Personal information* that it holds from an individual within 30 days after the request is received.

TDIF Req: PRIV-03-12-03; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* give the *Individual* access to their *Personal information* in the manner requested by the *Individual*, if it is reasonable, secure and practicable to do so.

TDIF Req: PRIV-03-12-04; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* provide access at no cost to the *Individual*.

TDIF Req: PRIV-03-12-05; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* where access is refused, take steps to meet the needs of the *Individual* and provide a written notice as set out in APP 12.

3.12.2 Correction

TDIF Req: PRIV-03-12-06; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* allow *Individuals* to correct their *Personal information* it holds as set out in *APP* 13.

TDIF Req: PRIV-03-12-07; **Updated**: Mar-20; **Applicability**: A, C, I
The *Applicant* *MUST* provide *Individuals* with a simple and accessible means to access and review their *Personal information.*

TDIF Req: PRIV-03-12-07a; **Updated**: Mar-20; **Applicability**: A, C, I
The *Applicant* MUST provide *Individuals* with a channel to update their *Personal information* in near to real time.

3.12.3 Individual history log

TDIF Req: PRIV-03-12-08; **Updated**: Mar-20; **Applicability**: X
The *Applicant* MUST provide *Individuals* with a centralised view of the metadata of services the *Individual* accessed, the time of access and the *Attributes* passed to the Relying Party unless such information has already been destroyed by the *Applicant* in accordance with the TDIF.

3.13 Quality of personal information

TDIF Req: PRIV-03-13-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
An *Applicant* MUST take reasonable steps to ensure quality of *Personal information* as outlined in *APP* 10.

TDIF Req: PRIV-03-13-02; **Updated**: Mar-20; **Applicability**: A, C, I
The *Applicant* MUST implement internal practices, procedures and systems (including training *Personnel* in these practices, procedures and systems) to audit, monitor, identify and correct poor-quality *Personal information*.

TDIF Req: PRIV-03-13-03; **Updated**: Mar-20; **Applicability**: A, C, I
The *Applicant* MUST ensure updated or new *Personal information* is promptly added to relevant existing records.

3.14 Handling Privacy Complaints

TDIF Req: PRIV-03-14-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* MUST provide a complaints service for handling privacy complaints which:

a) is readily accessible, including prominent contact information about the service.
b) is fair, including a process that is impartial, confidential and transparent.

c) has a process that is timely, clear and can provide a remedy where applicable.
d) has skilled and professional people who have knowledge of privacy laws and these *TDIF* privacy requirements and the complaint service process.
e) is integrated with other complaint handling bodies, (e.g. other *Participants* of an identity federation) as required, so it can assist the individual and refer complaints.

3.15 Destruction and de-identification

TDIF Req: PRIV-03-15-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* demonstrate it takes reasonable steps to destroy or de-identify *Personal information* in line with *APP* 11.2.

4 Protective Security Requirements

Several requirements listed in this section align with security advice, guidance, policies and publications developed by the Australian Government. This includes the *Australian Government Protective Security Policy Framework* (*PSPF*)[6] and *AGIS* developed by the *Australian Government Attorney General's Department* and *Australian Government Information Security Manual* (*ISM*)[7] developed by the *Australian Cyber Security Centre* (*ACSC*). These requirements ensure *Applicants* establish a minimum protective security baseline for their identity service.

Applicants that undergo the *TDIF Accreditation Process* should note the following:

- Refences to 'entities', 'agencies', 'accountable authority', 'Australian Government' in the *PSPF*, *AGIS* or *ISM* are to be interpreted as references to the *Applicant*.
- References to *PSPF*, *AGIS* or *ISM* controls that are applicable to an agency are to be interpreted as being applicable to the *Applicant*.
- The scope of *PSPF*, *AGIS* or ISM controls are limited to the identity service being accredited and not to the *Applicant's* wider operating environment.
- At a minimum the *Applicant* must handle all information as *OFFICIAL information* unless the *Applicant* has determined a higher security classification is required. See the *PSPF* (INFOSEC-08 - Sensitive and classified information) for further information on the sensitive and security classification of information.

To the extent of any conflict between:

- Any requirement in these *TDIF* protective security requirements and the current edition of the *PSPF*, then the *PSPF* takes precedence.
- Any requirement listed in these *TDIF* protective security requirements and the current edition of the *ISM*, then the *ISM* takes precedence.
- Any requirement in these *TDIF* protective security requirements and the current edition of the *AGIS*, then the *AGIS* takes precedence.

6 A copy of the *PSPF* is available at https://www.protectivesecurity.gov.au/

7 A copy of the *ISM* is available at https://www.cyber.gov.au/ism

4.1 Security governance

Security governance ensures each *Applicant* manages security risks and supports a positive security culture in an appropriately mature manner which ensures:

- Clear lines of accountability.
- Sound security planning.
- Investigation and response.
- Assurance and review processes.
- Proportionate reporting.

4.1.1 Role of the Accountable Authority

The following is taken from the *PSPF* (GOVSEC-01 - Role of the Accountable Authority).

TDIF Req: PROT-04-01-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* MUST appoint a senior executive as the designated *Accountable Authority* for managing security risks within their organisation.
TDIF Req: PROT-04-01-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Accountable Authority* MUST:

a) Determine the *Applicant's* tolerance for security risks.
b) Manage the *Applicant's* security risks.
c) Demonstrate how its protective security controls are applied to its identity system.
d) Consider the implications their risk management decisions have for other agencies and organisations and share information on risks where appropriate.

TDIF Req: PROT-04-01-03; **Updated**: Mar-20; **Applicability**: A, C, I, X
Where exceptional circumstances prevent or affect the *Applicant's* capability to implement a TDIF requirement, the *Accountable Authority*:

a) *MUST* record the decision to vary its security arrangements and advise the DTA of remedial action taken to reduce the risk to their business operations. These decisions will be requested by the *DTA* during *Annual Assessments*.
b) *MAY* vary application, for a limited period of time, consistent with the *Applicant's* risk tolerance.

4.1.2 Management structures and responsibilities

The following is taken from the *PSPF* (GOVSEC-02 - Management structures and responsibilities).

TDIF Req: PROT-04-01-04; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Accountable Authority MUST* appoint a *Chief Security Officer* (*CSO*) at a management level to be responsible for security in the *Applicant's* organisation.

TDIF Req: PROT-04-01-04a; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Accountable Authority MUST* empower the *CSO* or equivalent role to make decisions about:

a) Appointing security advisors with the *Applicant's* organisation.
b) The *Applicant's* protective security planning.
c) The *Applicant's* protective security practices and procedures.
d) Investigating, responding to and reporting on security incidents.

TDIF Req: PROT-04-01-05; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Accountable Authority MUST* ensure *Personnel* are aware of their collective responsibility to foster a positive security culture and are provided sufficient information and training to support this.

TDIF Req: PROT-04-01-05a; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *CSO* or equivalent role *MUST* be responsible for directing all areas of security to protect the *Applicant's Personnel*, Information, *ICT* and assets. This includes appointing security advisors to support them in the day-to-day deliver of protective security and to perform specialist services as required.

TDIF Req: PROT-04-01-06; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* develop and use procedures that ensure:

a) All elements of the *Applicant's System Security Plan* are achieved.
b) *Cyber security incidents* are investigated, responded to and reported to the *Oversight Authority* and *DTA*.
c) Relevant security policy or legislative obligations are met.

TDIF Req: PROT-04-01-07; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* provide all *Personnel* with security awareness training at engagement and annually thereafter. A copy of these training materials will be requested by the *DTA* as part of initial accreditation and annually thereafter as part of the *Annual Assessment*.

TDIF Req: PROT-04-01-08; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* maintain appropriately documented instructions and procedures to assist *Personnel* prevent, detect, report and deal with security risks.

TDIF Req: PROT-04-01-09; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* provide *Personnel* in specialist and high-risk positions (including contractors and security incident investigators) with specific security awareness training targeted to the scope and nature of the position.

TDIF Req: PROT-04-01-10; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* maintain a monitored email address as a central conduit for all security-related matters across governance, *Personnel*, information, *ICT* and physical security.

TDIF Req: PROT-04-01-11; **Updated**: Mar-20; **Applicability**: A, C, I
The *Applicant* *MUST* provide security advice to users on how to safeguard their *Digital Identity*, *Credentials*, *Personal information* and *Attributes*.

4.1.3 Security risk assessments

The following is taken from the *PSPF* (GOVSEC-03 - Security planning and risk management).

TDIF Req: PROT-04-01-12; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* have in place a *System Security Plan* approved by the *Accountable Authority* to manage the *Applicant's* security risks.

TDIF Req: PROT-04-01-12a; **Updated**: Mar-20; **Applicability**: A, C, I, X
The System *Security Plan* *MUST* include:

a) Security goals and strategic objectives of the *Applicant*, including how security risk management intersects with and supports broader business objectives and priorities.
b) *Applicant's* strategies to implement security risk management and maintain a positive risk culture.
c) *Applicant's* tolerance to security risks.
d) Maturity of the *Applicant's* capability to manage security risks.
e) A summary of the threats, risks and vulnerabilities that impact the confidentiality, integrity and availability of the *Applicant's* identity service.
f) Treatment strategies and controls put in place to manage security risks and vulnerabilities.
g) Strategies to ensure the *Applicant* meets its training and awareness needs.
h) Procedures and mechanisms for security incident management, security investigations and reporting security incidents.
i) An outline of key roles and responsibilities for protective security control within the *Applicant's* organisation.

Where a *Single Security* Plan is not practicable due to the *Applicant's* side or complexity of business, the *Accountable Authority* may approve a strategic-level overarching *System Security Plan* that addresses the requirements listed above.

TDIF Req: PROT-04-01-13; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *System Security Plan* (and supporting *System Security Plans*) *MUST* be reviewed annually by the *Applicant's Accountable Authority* and when there is a substantial change in the structure, functions or activities of the *Applicant* which impact the operation of the protective security components of their identity system.

TDIF Req: PROT-04-01-13a; **Updated**: Mar-20; **Applicability**: A, C, I, X
This review *MUST*:

a) Determine the adequacy of existing protective security control measures and mitigation controls.
b) Respond to and manage significant shifts in the *Applicant's* risk, threat and operating environment.

TDIF Req: PROT-04-01-14; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* identify *Personnel*, information, *ICT* and assets that are critical to the ongoing operation of the *Applicant's* identity system and apply appropriate protections to these resources to support their operation.

TDIF Req: PROT-04-01-15; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* identify a risk steward (or manager) who is responsible for each security risk or category of security risk, including for shared risks.

TDIF Req: PROT-04-01-16; **Updated**: Mar-20; **Applicability**: A, C, I, X
When conducting a *Security assessment*, the *Applicant* *MUST* communicate to the affected organisation any identified risks that could potentially impact on their business operations.

TDIF Req: PROT-04-01-17; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *System Security Plan* (and supporting *System Security Plans*) *MUST* include scalable measures to meet variations in threat levels and accommodate changes in the *National Terrorism Threat Level*.

TDIF Req: PROT-04-01-18; **Updated**: Mar-20; **Applicability**: A, C, I, X
Where the *CSO* (or security advisor on behalf of the *CSO*) implements an alternative mitigation measure or control to a *TDIF* requirement, they *MUST* document the decision and adjust the maturity level for the related *TDIF* requirement. These decisions will be requested by the *DTA* during *Annual Assessments*.

4.1.4 Security maturity monitoring

The following is taken from the *PSPF* (GOVSEC-04 - Security maturity monitoring).

TDIF Req: PROT-04-01-19; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant MUST* assess the maturity of its security capability and risk culture by considering its progress against goals and strategic objectives identified in its *System Security Plan*.

TDIF Req: PROT-04-01-19a; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant MUST* document and evidence their assessment of its security maturity.

4.2 Information security

Information security ensures each *Applicant* maintains the confidentiality, integrity and availability of all information it handles.

4.2.1 Sensitive and classified information

The following is taken from the *PSPF* (INFOSEC-08 - Sensitive and classified information).

TDIF Req: PROT-04-02-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant MUST*:

a) Identify information holdings.
b) Assess the sensitivity of information holdings.
c) Implement operational controls for these information holdings proportional to their value, importance and sensitivity.

TDIF Req: PROT-04-02-02; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant MUST* ensure information it holds is stored, transferred, transmitted and disposed of securely in a manner that meet the minimum protection requirements set out in the PSPF[8]. This includes ensuring *Sensitive information* is appropriately destroyed or archived when it has passed minimum retention requirements or reaches authorised destruction dates.

8 See *INFOSEC-01 - sensitive and classified information* Annexes A to D for further details.

4.2.2 Access to information

The following is taken from the *PSPF* (INFOSEC-09 - Access to information).

TDIF Req: PROT-04-02-03; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* enable appropriate access to information. This includes:

a) Sharing information within the *Applicant's* organisation as well as with other relevant stakeholders as required.
b) Ensuring that access to *Sensitive information* or resources is only provided to people with a *Need to know* that information.
c) Controlling access (including remove access) to supporting ICT systems, networks, infrastructure, devices and applications.

TDIF Req: PROT-04-02-04; **Updated**: Mar-20; **Applicability**: A, C, I, X

To manage access to information systems holding *Sensitive information*, the *Applicant* *MUST* implement unique *User* identification, authentication and authorisation practices on each occasion where system access is granted.

4.2.3 Safeguarding information from cyber threats

The following is taken from the *PSPF* (INFOSEC - 10 - Safeguarding information from cyber threats).

TDIF Req: PROT-04-02-05; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* mitigate common and emerging cyber threats by implementing the *ASD Strategies to Mitigate Cyber Security Incidents.*

TDIF Req: PROT-04-02-05a; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MAY* consider implementing additional *ASD Strategies to Mitigate Cyber Security Incidents*.

TDIF Req: PROT-04-02-06; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST NOT* expose the public to unnecessary security risks when transacting online.

4.2.4 Incident management, investigations and reporting

TDIF Req: PROT-04-02-07; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* implement a mechanism for detecting *Cyber security incidents*, including a process for *Personnel* and *Users* to report suspected *Cyber security incidents* confidentially.

TDIF Req: PROT-04-02-08; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* implement a control mechanism to flag *Cyber security incidents*.

TDIF Req: PROT-04-02-08a; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* compare all new registrations and updates to existing records against the control mechanism used to flag *Cyber security incidents*.

TDIF Req: PROT-04-02-08b; **Updated**: Mar-20; **Applicability**: A, C, I

The *Applicant* *MUST NOT* allow a new registration or update to be completed if the control mechanism indicates the registration or update will create a *Cyber security incident*.

TDIF Req: PROT-04-02-09; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* maintain documented procedures setting out criteria for making decisions at critical stages in managing *Cyber security incidents*.

TDIF Req: PROT-04-02-10; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* take responsibility for investigating *Cyber security incidents*, including investigating disciplinary matters, unless the matter is referred to and accepted by the *AFP* or another law enforcement agency.

TDIF Req: PROT-04-02-11; **Updated**: Mar-20; **Applicability**: A, C, I, X

Where a law enforcement agency declines a referral, the *Applicant* *MUST* resolve the matter in accordance with relevant internal and external requirements.

TDIF Req: PROT-04-02-12; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* refer all instances of potential or serious or complex security offences to the *AFP* in accordance with the *AGIS* and *AFP* referral process, except in the following circumstances:

a) Where legislation sets out specific alternative arrangements.
b) Where the *Applicant*:
    iii. Has the capacity and the appropriate skills and resources needed to investigate potential criminal matters.
    iv. Meets the requirements of the *AGIS* for gathering evidence and the *CDPP* in preparing briefs of evidence.

TDIF Req: PROT-04-02-13; **Updated**: Mar-20; **Applicability**: A, C, I, X
Security investigations *MUST* be carried out by appropriately qualified personnel as set out in the *AGIS*. If external investigators are engaged, they must as a minimum meet the investigations competency requirements set out in the *AGIS*.

TDIF Req: PROT-04-02-14; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant MUST* take all reasonable measures to recover financial losses caused by illegal activity through proceeds of crime and civil recovery processes or administrative remedies.

TDIF Req: PROT-04-02-15; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant MUST* develop and use procedures to report *Cyber security incidents* to the *Oversight Authority* and *DTA*.

TDIF Req: PROT-04-02-15a; **Updated**: Mar-20; **Applicability**: A, C, I, X
As soon as they become aware the *Applicant MUST* report *Cyber security incidents* to the *Oversight Authority* and *DTA*.

TDIF Req: PROT-04-02-15b; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant MUST* include the following information when reporting *Cyber security incidents*:

a) Date and time of the *Cyber security incident*.
b) Quantity of *Cyber security incidents* and their level of severity.
c) Time taken to respond to the *Cyber security incident*.
d) Measures taken in response to the *Cyber security incident*.
e) If applicable, the *Identity Proofing Level* and *Credential Level* of the impacted identity record(s).
f) Any other supporting information (e.g. attack vectors used).

Depending on the nature of the *Cyber security incident* and legal advice sought, the *Oversight Authority* and *DTA* may advise impacted stakeholders of the outcome of a security investigation.

TDIF Req: PROT-04-02-16; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* develop and use procedures to report significant *Cyber security incidents* to the relevant authority or affected entity as described in the *PSPF*[9].

4.2.5 Support for victims of security incidents

TDIF Req: PROT-04-02-17; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* implement a process which allows users to notify them when they suspect or become aware of a *Cyber Security Incident*.

TDIF Req: PROT-04-02-18; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* provide (either directly or through a third party) support services to *Users* who are impacted by *Cyber security incidents*.

TDIF Req: PROT-04-02-19; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* have in place processes such as appropriate identification of an *Individual* whose *Attributes*, *Digital Identity* or *Credential* has been subject to a *Cyber Security Incident* and appropriate technologies to enable the *Applicant* to flag the *Attributes*, *Digital Identity* or *Credential* as compromised.

TDIF Req: PROT-04-02-20 **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* prevent the continued use of a *User's Attributes*, *Digital Identity* or *Credentials* once the *Applicant* suspects or it becomes aware it has been subject to a *Cyber Security Incident*.

TDIF Req: PROT-04-02-20a; **Updated**: Mar-20; **Applicability**: I
When an *Individual* is identified by the *Applicant* as a victim of a *Cyber Security Incident*, or the *Individual* self-identifies, their existing *EoI documents* *MUST* be reproofed to the highest *Identity Proofing Level* which they have previously met.

9 See *GOVSEC 02 - Requirements for reporting security incidents* for further details.

TDIF Req: PROT-04-02-20b; **Updated**: Mar-20; **Applicability**: C

When an *Individual* is identified by the *Applicant* as a victim of a *Cyber Security Incident*, or the *Individual* self-identifies, their *Credential* *MUST* be reverified to the highest *Credential Level* which they have previously met.

TDIF Req: PROT-04-02-20c; **Updated**: Mar-20; **Applicability**: A

When an *Individual* is identified by the *Applicant* as a victim of a *Cyber Security Incident*, or the *Individual* self-identifies, their *Attributes* *MUST* be reverified.

4.2.6 Robust ICT systems

The following is taken from the *PSPF* (INFOSEC - 11 – Robust ICT systems).

TDIF Req: PROT-04-02-21; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* have in place secure measures during all stages of *ICT* systems development. This includes certifying and accrediting *ICT* systems in accordance with the *ISM* (or a similar process for non-government *Applicants*) when implemented into the operational environment.

TDIF Req: PROT-04-02-22; **Updated**: Mar-20; **Applicability**: A, C, I, X

When establishing new *ICT* systems or implementing improvements to current *ICT* systems (including software development), the *Applicant* *MUST* address security in the early phases of the system's development life cycle. This includes during the system concept development and planning phases, and then in the requirements analysis and design phases.

TDIF Req: PROT-04-02-23; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST NOT* process, store or communicate *Sensitive information* on an *ICT* system, unless the residual security risks to the system and information have been recognised and accepted by the *Accountable Authority*, *CSO* or a security advisor on behalf of the *CSO*.

TDIF Req: PROT-04-02-24; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* ensure their *ICT* systems (including software) incorporate processes for audit trails and activity logging in applications

TDIF Req: PROT-04-02-24a; **Updated**: Mar-20; **Applicability**: A, C, I, X

At a minimum activity logging *MUST* occur for the following events:

- Successful and failed elevation of privileges by *Personnel*.
- User and group additions, deletions and modification to permissions.
- Security related system alerts and failures (e.g. attempted access that is denied, crashes or error messages).
- Unauthorised access attempts to critical systems and files.
- The source *IP* address of the device that authenticated to the identity system.
- The source port used to perform the authentication event.
- The destination *IP* address used to perform the authentication event.
- The destination port used to perform the authentication event.
- The *User Agent String* which identifies the browser and operating system of the attempted authentication.
- The *International Mobile Equipment Identity* (*IMEI*) of a mobile phone (if a mobile phone is used to authenticate to the identity system).

TDIF Req: PROT-04-02-24b; **Updated**: Mar-20; **Applicability**: A, C, I, X

At a minimum activity logs *MUST* include:

- The date and time of the event,
- The relevant *User*, identifier or process. Each event must have a unique identifier.
- The event description.
- The *ICT* equipment involved.

Further guidance on events to log is available in the *ISM*.

TDIF Req: PROT-04-02-24c; **Updated**: Mar-20; **Applicability**: C

Activity logs *MUST* include:

- *Credential* type used.
- *Credential Level* achieved.

TDIF Req: PROT-04-02-24d; **Updated**: Mar-20; **Applicability**: I

Activity logs *MUST* include:

- *Identity Proofing Level* achieved.

TDIF Req: PROT-04-02-25; **Updated**: Mar-20; **Applicability**: A, C, I, X

Activity logs *MUST* be:

- Protected and stored to ensure the accuracy and integrity of data captured or held.
- Protected from unauthorised access, modification and deletion.
- Retained for a minimum of 7 years.
- Used to correlate activity across event logs, prioritise assessments and focus investigations.

4.2.7 Disaster recovery and business continuity management

TDIF Req: PROT-04-02-26; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* maintain a *Disaster Recovery and Business Continuity Plan* for its identity system that covers:

a) Business continuity governance.

b) Training requirements for recovery team members.

c) Recovery objectives and priorities.

d) Continuity strategies.

e) Testing requirements and restoration procedures.

TDIF Req: PROT-04-02-27; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* test their *Disaster Recovery and Business Continuity Plan* annually. The *DTA* will request evidence of as part of accreditation and during *Annual Assessments*.

4.2.8 Cryptography

TDIF Req: PROT-04-02-28; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* use:

- *Australian Signals Directorate Approved Cryptographic Algorithms* (*AACAs*).
- *Australian Signals Directorate Approved Cryptographic Protocols* (*AACPs*).

To protect information while in transit and at rest.

TDIF Req: PROT-04-02-29; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* maintain a *Cryptographic Key Management Plan* for their identity system which covers:

a) Cryptographic key lifecycle management over the lifecycle of the key (generation, delivery, renewal, revocation, etc).
b) How records will be maintained and audited.
c) The conditions under which compromised keys will be declared.
d) Maintenance of cryptographic components.
e) Evidence of cryptographic evaluations undertaken.

4.3 Personnel security

Personnel security enables each *Applicant* to ensure its *Personnel* are suitable to access information (including *ICT*) and assets and meet an appropriate standard of integrity and honesty

4.3.1 Eligibility and suitability of personnel

The following is taken from the *PSPF* (PERSEC - 12 – Eligibility and suitability of personnel).

TDIF Req: PROT-04-03-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* ensure the eligibility and suitability of its *Personnel* who have access to information, *ICT* and assets which support the operation of their identity service.

TDIF Req: PROT-04-03-02; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* undertake pre-employment screening on people, including:

a) Verifying *Identity* using the *Document Verification Service*.
b) Confirming eligibility to work in Australia.

4.3.2 Ongoing assessment of personnel

The following is taken from the *PSPF* (PERSEC - 13 – Ongoing assessment of personnel).

TDIF Req: PROT-04-03-03; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* assess and manage the ongoing suitability of its *Personnel*.

4.3.3 Separating personnel

The following is taken from the *PSPF* (PERSEC - 14 – Separating personnel).

TDIF Req: PROT-04-03-04; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* ensure that separating *Personnel* have their access to the *Applicant's* resources withdrawn, including:

a) Physical facilities.
b) ICT systems.

TDIF Req: PROT-04-03-05; **Updated**: Mar-20; **Applicability**: A, C, I, X

Prior to *Personnel* separation or transfer, the *Applicant* *MUST* ensure the *CSO*, or relevant security advisor is advised of any proposed cessation of employment resulting from misconduct or other adverse reasons.

TDIF Req: PROT-04-03-05a; **Updated**: Mar-20; **Applicability**: A, C, I, X

Where it is not possible to undertake required separation procedures, the *Applicant* *MUST* undertake a risk assessment to identify any security implications.

4.4 Physical security

Physical security provides a safe and secure physical environment for their *Personnel*, information and assets.

4.4.1 Physical security for Applicant resources

The following is taken from the *PSPF* (PHYSEC - 15 – Physical security for entity resources).

TDIF Req: PROT-04-04-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* implement physical security measures that minimise or remove the risk of:

a) Harm to *Individuals*.
b) Information and physical assets and resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

TDIF Req: PROT-04-04-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* protect its resources commensurate with the assessed business impact level of their compromise, loss or damage.

TDIF Req: PROT-04-04-03; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* assess security risks and select appropriate containers, cabinets, secure rooms and strong rooms to protect information and assets.

TDIF Req: PROT-04-04-04; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* dispose of physical assets securely.

5 User Experience Requirements

5.1 Usability requirements

TDIF Req: UX-05-01-01; **Updated**: Mar-20; **Applicability**: A, C, I

The *Applicant* *MUST* demonstrate how *Users* can also use other available channels if needed, without repetition or confusion.

TDIF Req: UX-05-01-02; **Updated**: Mar-20; **Applicability**: A, C, I

The *Applicant* *MUST* demonstrate how *Users* with low digital skills can have readily available access to *Assisted Digital* support.

TDIF Req: UX-05-01-03 **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* demonstrate how its identity system is built with responsive design methods to support common devices, browsers and assistive technologies, including desktop and mobile devices.

TDIF Req: UX-05-01-04; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* allow *Users* to provide feedback, seek assistance or otherwise resolve disputes or complaints in relation to the *Applicant's* identity system.

TDIF Req: UX-05-01-05; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* create and maintain an individual end-to-end journey map[10] for its identity system.

TDIF Req: UX-05-01-05a; **Updated**: Mar-20; **Applicability**: I

Where the *Applicant* cannot support a *User's* technology preference, the individual journey map *MUST* indicate how an Individual can use an alternative channel to complete a specific activity.

[10] An Individual journey map is a visualization or diagram (or several diagrams) that depict the stages, and interfaces, that a person goes through when interacting with the identity system in order to accomplish their goal.

TDIF Req: UX-05-01-06; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* ensure information it provides to *Users* is available in multiple accessible formats, including accessible online formats (such as *HTML*), large print format, *Easy English*, and braille (on request).

TDIF Req: UX-05-01-07; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* provide *Users* with uncomplicated ways to learn about its identity system on digital channels.

5.2 Requirements for the identity verification journey

TDIF Req: UX-05-02-01; **Updated**: Mar-20; **Applicability**: I

The *Applicant* *MUST* provide *Users* with information about the entire identity management process, including what to expect in each step of the individual journey and what they will need to do in order to complete each step.

TDIF Req: UX-05-02-02; **Updated**: Mar-20; **Applicability**: I

The *Applicant* *MUST* provide *Users* with information on technical requirements for using the *Applicant's* identity system (for example, requirements for internet access, or access to a mobile phone or webcam).

TDIF Req: UX-05-02-03; **Updated**: Mar-20; **Applicability**: I

The *Applicant* *MUST* provide *Users* with information on the required *Identity documents*, whether each piece is mandatory, and the consequences for not providing the complete set of required documents. Individuals need to know the specific combinations of identity documents.

TDIF Req: UX-05-02-04; **Updated**: Mar-20; **Applicability**: I
If a code or number is issued by the *Applicant* to a *User* as part of the identity verification process, the *Applicant* *MUST* notify the *User* in advance that they will receive a digital code or number and what to do with it.

TDIF Req: UX-05-02-05; **Updated**: Mar-20; **Applicability**: I
The *Applicant* *MUST* advise the *User* whether the identity verification process has been successfully completed.

TDIF Req: UX-05-02-05a; **Updated**: Mar-20; **Applicability**: I

If verification is successful, the *Applicant* *MUST* send the *User* confirmation regarding the successful verification and information on next steps.

TDIF Req: UX-05-02-05b; **Updated**: Mar-20; **Applicability**: I

If verification is partially complete[11], the *Applicant* *MUST* communicate to the *User* what information will be discarded.

TDIF Req: UX-05-02-05c; **Updated**: Mar-20; **Applicability**: I

If verification is unsuccessful, the *Applicant* *MUST* provide the *User* with information for alternative options, for example, offering an over-the-counter identity verification process if they were unable to complete the digital identity verification process.

TDIF Req: UX-05-02-06; **Updated**: Mar-20; **Applicability**: I

The *Applicant* *MUST* provide support to *Users* who need assistance during the identity verification process.

TDIF Req: UX-05-02-07; **Updated**: Mar-20; **Applicability**: I

The *Applicant* *MUST* provide support to *Users* who do not have the technology or capacity to create a *Digital Identity*. For example, by providing support via a shopfront, a call centre that is contactable via the *National Relay Service*, or through a text-based support such as an online chat window.

TDIF Req: UX-05-02-08; **Updated**: Mar-20; **Applicability**: I

The *Applicant* *MUST* provide clear instructions to a *User* on how they can update their *Personal information* collected as part of the identity verification process.

5.3 Requirements for the authentication journey

TDIF Req: UX-05-03-01; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* provide *Users* with relevant information for the use and maintenance of their *Credential*. For example, this may include instructions for use, information on *Credential* expiry, and what to do if the *Credential* is forgotten, lost or stolen.

11 A partially complete identity verification may occur due to *Individuals* not having the complete set of *Identity documents*, *Individual's* choosing to stop the process, or session timeouts.

TDIF Req: UX-05-03-02; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* enable *Users* to recover a *Credential* if it has been lost or forgotten. Additionally, the recovery mechanism must be as strong as the initial *Credential* provisioning process.

5.4 Usability test plans

TDIF Req: UX-05-04-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* document, by way of a *Usability Test Plan*, how it will conduct usability testing.

TDIF Req: UX-05-04-01a; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant's Usability Test Plan* *MUST*:

a) Describe the test objectives, usability goals, and usability metrics that will be captured.
b) Describe the number of test participants, how they will be recruited and the cohort to which they belong.
c) Document the approach and the methodology used to conduct the tests to indicate what is working, pain points and where improvements are needed.
d) Document representative scenarios for testing, on both desktop and mobile devices.
e) Describe how findings from usability testing will be implemented.
f) Identify a range of representative *Individuals* of the identity system.

TDIF Req: UX-05-04-01b; **Updated**: Mar-20; **Applicability**: A, C, I, X

The range of representative *Individuals* *MUST* include:

a) *Individuals* with disability.
b) Older *Individuals*.
c) *Individuals* who use assistive technologies.
d) *Individuals* with low literacy.
e) *Individuals* from culturally and linguistically diverse backgrounds.
f) *Individuals* who are Aboriginal or Torres Strait Islander.
g) *Individuals* from regional and remote areas.
h) *Individuals* with older technology and low bandwidth connections.

TDIF Req: UX-05-04-01c; **Updated**: Mar-20; **Applicability**: A, C, I, X

The range of representative *Individuals* *MUST* be gender neutral.

5.5 Conduct usability testing

TDIF Req: UX-05-05-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* use experienced *User Researchers* to conduct usability testing of its identity service. For the purpose of this requirement, an experienced *User Researcher* is highly skilled in identifying individual needs, conducting usability tests, and feeding insights back to the product team.

TDIF Req: UX-05-05-02; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* conduct usability testing on its identity system as part of initial accreditation and annually thereafter as part of the *Annual Assessment*.

TDIF Req: UX-05-05-03; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* conduct usability testing of its identity system from end to end, in an environment that replicates its live environment with a range of representative *Individuals*.

TDIF Req: UX-05-05-04; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* document the outcomes of its usability testing, including test methodology(s), test results, findings and recommendations.

TDIF Req: UX-05-05-04a; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* provide the outcomes of its usability testing to the *DTA* as part of initial accreditation and annually thereafter as part of the *Annual Assessment*.

5.6 Accessibility requirements

TDIF Req: UX-05-06-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant's* identity system *MUST* be presented in a clear and concise manner, using plain language that is easy to understand and accessible across all devices.

6 Technical testing requirements

6.1 Technical test planning

TDIF Req: TEST-06-01-01**; Updated:** Mar-20**; Applicability:** A, C, I, X
The *Applicant MUST* develop at least one *Technical Test Plan* which covers the testing of all applicable TDIF requirements (i.e. at a minimum the TDIF requirements set out at TEST-06-01-04).

TDIF Req: TEST-06-01-02**; Updated:** Mar-20**; Applicability:** A, C, I, X
The *Applicant MUST* include the content described in Table 1 in *Technical Test Plan* and provide a copy of the *Technical Test Plan* to the DTA as part of initial accreditation.

TDIF Req: TEST-06-01-03**; Updated:** Mar-20**; Applicability:** A, C, I, X
The *Applicant MUST* agree on test completion criteria with the DTA prior to commencing technical testing.

TDIF Req: TEST-06-01-04**; Updated:** Mar-20**; Applicability:** A, C, I, X
The *Applicant MUST* demonstrate through testing how its identity system meets the following TDIF requirements:

- Its *fraud* control mechanism for detecting incidents of *fraud* or suspected *fraud* (as per FRAUD-02-04-01).
- Its *fraud* control mechanism to flag incidents of *fraud* or suspected *fraud* (as per FRAUD-02-04-02).
- Its security mechanism for detecting *Cyber security incidents* (as per PROT-04-02-07).
- Its security mechanism to flag *Cyber security incidents* (as per PROT-04-02-08).
- Its processes for audit trails and activity logging in applications (as per PROT-04-02-24)
- The activities and events logged (as per PROT-04-02-24a)
- The content included in activity logs (as per PROT-04-02-24b)

TDIF Req: TEST-06-01-05**; Updated:** Mar-20**; Applicability:** A, C, I
The *Applicant* *MUST* demonstrate through testing how its identity system meets the following TDIF requirements:

- Its *fraud* control mechanism which prevents new registrations or updates to existing records from occurring if the *fraud* control mechanism indicates the registration or update is fraudulent or suspected of being fraudulent (as per FRAUD-02-04-02b).
- Its security mechanism which prevents new registrations or updates to existing records from occurring if the security mechanism indicates the registration or update will create a *Cyber security incident* (as per PROT-04-02-08b).

TDIF Req: TEST-06-01-06**; Updated:** Mar-20**; Applicability:** I
The *Applicant* *MUST* demonstrate through testing of all verification methods and *Identity Proofing Levels* its identity system supports as well as its *Step-Up* process if this is also supported.

TDIF Req: TEST-06-01-07**; Updated:** Mar-20**; Applicability:** C
The *Applicant* *MUST* demonstrate through testing all *Credential Levels* and *Credentials* its identity system supports as well as its *Step-Up* process if this is also supported.

TDIF Req: TEST-06-01-08**; Updated:** Mar-20**; Applicability:** A, C, I, X
The *Applicant* *MUST* develop a *Requirements Traceability Matrix* (RTM) which maps test cases to requirements, which *MUST* include all requirements the *Applicant* is required to do technical testing for.

Table 1: Technical Test Plan contents

Section	Details
Scope	Describes the coverage of the testing, including: • Inclusions. • Exclusions. • Limitations.
References	List of test references, including: *TDIF* requirements
Test scope	A summary of the items under test, including: • Features. • Attributes.

Section	Details
	• Interfaces. • Functions.
Assumptions, limitations and dependencies	Describes the assumptions, limitations and dependencies relevant to the *Technical Test Plan*.
Test approach	Describes the approach for testing each requirement and includes any automated testing.
Test incident and defect management	Describes how any test incident (where the actual execution result does not match the expected result) will be managed, the analysis of a test incident and the raising and management of any incident considered to be a defect.
Test entry	Describes the criteria used by the *Applicant* to assess whether they are ready to enter testing and the assessment undertaken to test these criteria prior to entry into testing.
Test exit	Describes the criteria used by the *Applicant* to assess whether they are ready to exit testing.
Test data	Describes the test data required for each phase of testing, the source and any security requirements, including as appropriate: Anonymisation of any production data where *Personal information* may be compromised. Simulated Data (where the interfacing system is not available for testing).
Test environment	Specifies the required test environment characteristics and set up process.
Test resources	Specifies the resources (equipment, applications, tools) required for testing activities.
Retesting and regression	Specifies the conditions under which retesting and regression testing is performed.
Suspension and resumption	Specifies the criteria for suspension of testing and the testing activities that may have to be repeated upon resumption.
Roles and responsibilities	Specifies the testing roles and the responsibilities assigned.
Test completion criteria	Describes the test completion criteria to be met for the *Applicant* to have completed testing activities.

6.2 Technical testing

TDIF Req: TEST-06-02-01**; Updated:** Mar-20**; Applicability:** A, C, I, X
The *Applicant MUST* be satisfied of the following prior to commencement of test execution:

a) The test plan is approved and released.
b) All requirements are included in the RTM.
c) All requirements are covered by one or more test cases.
d) All test cases are appropriately documented.
e) All test resources are identified and available.

TDIF Req: TEST-06-02-02**; Updated:** Mar-20**; Applicability:** A, C, I, X
The *Applicant MUST* assess and report execution coverage for each test case during the testing process.

6.3 Technical test completion

TDIF Req: TEST-06-03-01**; Updated:** Mar-20**; Applicability:** A, C, I, X
For test completion the *Applicant MUST* complete a *Technical Test Report* and provide this to the DTA as part of initial accreditation.

TDIF Req: TEST-06-03-02**; Updated:** Mar-20**; Applicability:** A, C, I, X
The *Applicant's Technical Test Report MUST* include:

a) Demonstration testing has been executed in accordance with the approved *Technical Test Plan*.
b) Status of all test cases, including the execution coverage and defects.
c) Test completion criteria has been met, where the criteria have not been met a risk-assessment must be included for approval to deviate and exit testing.

7 Functional Assessments

The *Applicant* is required to undergo a series of *Functional Assessments* by *Assessors*. These *Functional Assessments* include:

- A *Privacy Impact Assessment*.
- A *Privacy assessment*.
- A *Security assessment*.
- A *Penetration test*.
- A *Web Content Accessibility Guidelines* (*WCAG*) assessment.

7.1 PIA and Privacy Assessment

TDIF Req: ASSESS-07-01-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* commission an *Assessor* to conduct a *Privacy Impact Assessment* on their identity system as part of accreditation.

TDIF Req: ASSESS-07-01-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
Once accredited, the *Applicant* *MUST* conduct a *Privacy Impact Assessment* on all high-risk projects related to their identity system.

TDIF Req: ASSESS-07-01-03; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Privacy Impact Assessment* conducted *MUST*:

a) Be undertaken early enough to influence the design of the identity system.
b) Reflect consultation with relevant stakeholders.
c) Include a description of the proposed identity system.
d) Map the identity system's personal information flows.
e) Include an analysis of risks of non-compliance with relevant privacy laws and *TDIF* privacy requirements.
f) Include an analysis of the impact of the project on the privacy of Individuals.
g) Include an analysis of whether privacy impacts are necessary or avoidable.
h) Include an analysis of possible mitigations to privacy risks.
i) Include recommendations

TDIF Req: ASSESS-07-01-04; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant's* identity system *MUST* undergo a *Privacy Assessment* (which is separate to and follows on from the *PIA*) as part of initial accreditation and annually thereafter as part of the *Annual Assessment*.

7.2 Security assessment and penetration test

TDIF Req: ASSESS-07-02-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant's* identity system *MUST* undergo a *Security assessment* by a security *Assessor* (or *IRAP Assessor* or other security professional) to identify security deficiencies as part of initial accreditation and annually thereafter as part of the *Annual Assessment*.
As per the *TDIF: 03 - Accreditation Process:*

- The *Statement of Applicability* forms the basis of the *Applicant's Security assessment*.
- For multi-entity systems, the scope of the *Security assessment MUST* include all security controls which contribute to meeting the *TDIF* protective security requirements.

TDIF Req: ASSESS-07-02-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant's* identity system *MUST* undergo a *Penetration test* as part of each major production release during initial accreditation and annually thereafter as part of the *Annual Assessment*.

TDIF Req: ASSESS-07-02-02a; **Updated**: Mar-20; **Applicability**: A, C, I, X
For multi-entity systems the scope of the *Penetration test MUST* include all security controls which contribute to meeting the *TDIF* protective security requirements.

7.3 Accessibility assessment

TDIF Req: ASSESS-07-03-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant's* identity system *MUST* at a minimum:

- For web-based identity services meet *WCAG* version 2.0 to the AA standard.

- For mobile-based identity services meet *WCAG* version 2.1 to the AA standard.

As part of initial accreditation and annually thereafter as part of the *Annual Assessment*[12].

7.4 Applicant obligations

TDIF Req: ASSESS-07-04-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* undergo each *Functional Assessment*.

TDIF Req: ASSESS-07-04-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* define the scope[13], objectives and criteria for each *Functional Assessment* and provide this to the *DTA* as part of its *Accreditation Plan*.

7.5 Assessor skills, experience and independence

TDIF Req: ASSESS-07-05-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* demonstrate to the *DTA* how the *Assessors* have relevant, reasonable and adequate experience, training and qualifications to conduct the *Functional Assessment*.

TDIF Req: ASSESS-07-05-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The Applicant *MUST* demonstrate to the *DTA* how the *Assessors*:

- Are independent from the development and operational teams of the *Applicant's* identity system.
- Do not possess a conflict of interest in performing the *Functional Assessment* on the *Applicant's* identity system.

12 The *DTA* encourages all *Applicants* and *Accredited Participants* to meet *WCAG* version 2.1 which provides updated guidance around accessibility.

13 In the context of the *Security assessment* this refers to the *Statement of Applicability*.

7.6 Assessment process

TDIF Req: ASSESS-07-06-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* ensure *Assessors* have access to and consider all relevant evidence provided by the *Applicant* to the *DTA*. This includes any responses by the *DTA* to questions which may have been asked.

TDIF Req: ASSESS-07-06-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* ensure *Assessors* conduct the *Functional Assessments*.

TDIF Req: ASSESS-07-06-03; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* use the compliance ratings listed in 'Appendix A: Compliance ratings' when determining areas of compliance and non-compliance with the requirements of the TDIF.

TDIF Req: ASSESS-07-06-04; **Updated**: Mar-20; **Applicability**: A, C, I, X
The Functional Assessments *MUST* include:

a) Documentation reviews.
b) Interviews with key personnel.
c) A run through of the Applicant's identity system.

TDIF Req: ASSESS-07-06-05; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Functional Assessment* *MAY* include a site visit to the *Applicant's* premises or other location where it provides services in connection with its identity system.

7.7 Functional Assessment Report

TDIF Req: ASSESS-07-07-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* ensure the *Assessors* document the outcomes of the assessment in a *Functional Assessment Report*.

TDIF Req: ASSESS-07-07-01a; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant's Accountable Authority* *MUST* respond in writing, to the recommendations outlined in the *Functional Assessment Report* including whether the recommendations are accepted, the reasons for any non-acceptance and the timeframe for implementation of the recommendations.

TDIF Req: ASSESS-07-07-02; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant's Functional Assessment Report* *MUST* include:

a) A summary of the activities performed during the *Functional Assessment*.

b) The date of and period covered by the *Functional Assessment Report*.

c) Name, role (or position) and contact details of the relevant *Accountable Authority* and point of contact within the *Applicant's* government agency or organisation.

d) Qualifications and basis of independence for all *Assessors* used.

e) Names and versions of all documents used by the *Applicant*.

f) City, state (and if applicable, country) of all physical locations used in the *Applicant's* operations. This includes data centre locations (primary and alternative sites) and all other locations where general ICT and business process controls that are relevant to the *Applicant's* operations are performed.

g) The test or evaluation methodology(s) used.

h) The test or evaluation results.

i) Findings.

j) Remediation actions or recommendations to address any areas of non-compliance.

k) Express an opinion and provide recommendations to the *DTA* of the *Applicant's* identity system against the *TDIF* requirements, including any requirements that could not be adequately assessed due to access or timing issues.

l) Include a list of compliant and non-compliant controls. Where a non-compliance has been identified, the remedial actions and timeframes within which the actions will be completed to address the non-compliance.

TDIF Req: ASSESS-07-07-03; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST*:

- Provide a copy of the full findings and report to the *DTA*, or
- Enable the *DTA* access to a copy of the findings and report.

An executive summary or redacted version of the findings or *Functional Assessment Report* is insufficient to meet this requirement.

Appendix A: Compliance ratings

The *Assessors* must use the following compliance ratings to indicate whether the *Applicant's* identity system meets *TDIF* requirements. Refer to the ISO 31000 or the *Applicant's* own risk management framework for a description of likelihood and consequence ratings.

- **Not Applicable (N/A)**. A *TDIF* requirement that does not apply to an *Applicant* as their identity system does not use, rely on or support the *TDIF* requirement (for example, *TDIF* requirements for elliptic curve cryptography will be N/A if the identity system supports other *AACAs* instead).
- **Compliant**. The *Applicant* has demonstrated with evidence they comply with a *TDIF* requirement or the intent of a requirement.
- **Critical Non-Compliance**. The *Applicant* fails to meet a *TDIF* requirement which may result in extreme unmitigated risk.
    - A critical non-compliance must be classified as a critical failure and must result in a failed *Functional Assessment*.
    - The immediate withdrawal of an existing accreditation may occur until such time as the critical non-conformance is addressed.
- **Major Non-Compliance**. The *Applicant* fails to meet a *TDIF* requirement which may result in high unmitigated risk.
    - A major non-compliance must be classified as a major failure and must result in a failed *Functional Assessment*.
    - Escalation of the problem to a critical failure must be imposed if additional events impact on the *Applicant* simultaneously.
    - If the *Applicant* fails to rectify the compliance problem within a timeframe agreed with the *DTA*, then the status of the problem must be escalated to a critical failure and the conditions of that category are then applied.
- **Partial Non-Compliance**. The *Applicant* fails to meet a *TDIF* requirement which may result in moderate unmitigated risk must be classified as a partial failure.
    - Escalation of the problem to a major failure must be imposed if additional failures within this category are detected.
    - If the *Applicant* fails to rectify the compliance problem within a timeframe agreed with the *DTA*, then the status of the problem must be escalated to a major failure and the conditions of that category are then applied.

- **Minor Non-Compliance**. The *Applicant* fails to meet a *TDIF* requirement which may result in low unmitigated risk should be classified as minor failures.
    - Escalation of the problem to a partial failure must be imposed if additional failures within this category are detected.
    - If the *Applicant* fails to rectify the compliance problem within a timeframe agreed with the *DTA*, then the status of the problem must be escalated to a partial failure where the conditions of that category are then applied.