Australian Government | Digital Identity

04 Functional Requirements

Trusted Digital Identity Framework

Release 4.8 - Feb 2023

PUBLISHED VERSION

Digital Transformation Agency (DTA)

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 you 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)™: 04 Functional Requirements © Commonwealth of Australia (Digital Transformation Agency) 2023

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 and 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 Providers*, 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 digitalidentity@dta.gov.au :

Document management

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

Change log

Document Version	Release 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	4.0	May 2020		Published version
1.1	4.1	January 2021	JK	CRID0005 – Emergency Change to ASSESS-07-03-01 (minor typo)
1.2	-	March 2021	JK, SJP	Consultation Version
1.3	4.4	June 2021	JK, SJP, MS, AV	CRID0007, CRID0009, CRID0015, CRID00018, CRID0023 – Changes to requirements, new requirements added, archived requirements: See TDIF Change Log for full list of requirements changes.
1.4	4.5	Oct 2021	JK, AV	CRID0027 – Emergency Change to PRIV-03-07-01a
1.5	4.6	March 2022	AV, JK, SJP, DN, MS	Applicability of requirements added. Improvements to structure and clarity. See TDIF Change Log for full list of requirements changes
NA	4.7	June 2022		No changes to document
NA	4.8	Feb 2023		No changes to document

All changes made to the TDIF are published in the TDIF Change Log which is available at https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework.

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 organisations or government agencies through other policies, legislation or regulations, or by any other means. These *TDIF functional requirements* supplement existing obligations and apply specifically to *Applicants* that undergo the *TDIF Accreditation Process* including, where relevant, an *Applicant's Identity System*.

The intended audience for this document includes:

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

2 Fraud Control Requirements

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

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.

2.1 Digital Identity Fraud Controller

TDIF Req: FRAUD-02-01-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST have an officer or senior employee of the *Applicant* as the designated *Digital Identity Fraud Controller* who is responsible for:

a) managing *Digital Identity Fraud Risks* within its organisation; and
b) ensuring the *Applicant* complies with the fraud control requirements in this section.[2]

TDIF Req: FRAUD-02-01-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST conduct an assessment of the *Digital Identity Fraud Risk* associated with the *Applicant's Identity System* prior to accreditation and at least once every 12 months beginning on the date the *Applicant* was accredited.

[2] For Commonwealth, State and Territory entities, this role can be fulfilled by their accountable authority.

TDIF Req: FRAUD-02-01-03; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST*:

a) Determine the *Applicant's* tolerance for *Digital Identity Fraud Risks*.
b) Manage the *Applicant's Digital Identity Fraud Risks*, including by complying with the requirements of this section.
c) Demonstrate how its *Digital Identity fraud* controls are applied to its *Identity Facility*.
d) Take all reasonable measures to prevent, detect and deal with *Digital Identity fraud* relating to its *Identity System*.
e) Consider the implications their risk management decisions have for *Accredited Providers, Relying Parties, Users* and other organisations and share information on risks with them where appropriate.

TDIF Req: FRAUD-02-01-04; **Updated**: Mar-22; **Applicability**: A, C, I, X

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

a) *MUST,* as soon as practicable notify the DTA of the circumstances and the non-compliance, including details of the remedial action (if any) taken or to be taken to reduce the risk to the *Applicant's Identity System*
b) *MUST* keep a record of decisions taken by the *Applicant* in relation to such non-compliance and remedial action (if any). These decisions will be requested by the *DTA* during *Annual Assessments*.
c) *MAY* vary the *Applicant's Digital Identity* fraud control arrangements (including, if relevant, the *Digital Identity Fraud Control Plan*) for a limited period, but not so as to increase the level of *Digital Identity Fraud Risk* above the *Applicant's* risk tolerance.

2.2 Digital Identity Fraud Control Plan

TDIF Req: FRAUD-02-02-01; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* have in place a *Digital Identity Fraud Control Plan* approved

by the *Digital Identity Fraud Controller* to manage the *Applicant's Digital Identity Fraud Risks*.[3]

TDIF Req: FRAUD-02-02-01a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Digital Identity Fraud Control Plan* MUST detail the:

a) Fraud control goals and strategic objectives of the *Applicant*, including how the management of *Digital Identity Fraud Risks* intersects with and supports broader business objectives and priorities.
b) *Applicant's* strategies to implement *Digital Identity Fraud Risk* management and maintain a positive risk culture.
c) *Applicant's* tolerance of *Digital Identity Fraud Risks*.
d) *Digital Identity Fraud* threats, risks and vulnerabilities that impact the protection of the *Applicant's Personnel*, information (including *ICT*) and assets used in connection with the services for which the *Applicant* is accredited.
e) Maturity of the *Applicant's* capability to manage *Digital Identity Fraud Risks*.
f) Treatment strategies and controls put in place to manage *Digital Identity fraud* threats, risks and vulnerabilities.
g) Strategies and controls to ensure the *Applicant* and its *Personnel* successfully complete appropriate training and raise awareness in relation to *Digital Identity Fraud Risks.*
h) Procedures and mechanisms for *Digital Identity Fraud Incident* management, *fraud* investigations and reporting *Digital Identity Fraud Incidents*.
i) An outline of key roles and responsibilities for *Digital Identity Fraud Control* within the *Applicant's* organisation.
j) The risk ratings and scale to be used by the *Applicant* when assessing the severity of a *Digital Identity Fraud Incident*.
k) Where applicable, details of the procedures to detect fraudulent activities by the *Assessing Officer* when performing *Manual Face Comparison*.
l) Where applicable, details of the *Applicant's* approach to the use of *Biometric Information*.

[3] An *Applicant's Digital Identity Fraud Control Plan* may be a component of an overall *fraud control plan* for the *Applicant*.

m) Where applicable, a description of the location(s) from which *Local Biometric Binding* will be undertaken by the *Applicant*.

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

The *Applicant MUST* review and update its *Digital Identity Fraud Control Plan*:

a) at least annually; and

b) as soon as practicable after:

i. the Applicant becomes aware of a Digital Identity Fraud Incident which is of a type not covered in the Applicant's Digital Identity Fraud Control Plan or which exceeds the Applicant's tolerance of Digital Identity Fraud Risks as set out in their Digital Identity Fraud Control Plan;

ii. the Applicant becomes aware of a breach of the requirements of their Digital Identity Fraud Control Plan;

iii. a change in the structure, functions or activities of the Applicant which may impact the operation of the fraud control components of their Identity System.

iv. a change to the Applicant's Identity System where such change may increase the level of Digital Identity Fraud Risk.

TDIF Req: FRAUD-02-02-02a; **Updated**: Mar-22; **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 Digital Identity Fraud prevention, awareness and training

TDIF Req: FRAUD-02-03-01; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant MUST* maintain records of instructions it gives its *Personnel* and contractors and procedures to assist *Personnel* to prevent, detect, report and deal with *Digital Identity Fraud Incidents*.

TDIF Req: FRAUD-02-03-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST provide appropriate *Digital Identity Fraud Risk* information and training to *Personnel* whose duties relate to the services for which the *Applicant* is accredited:

a) before such *Personnel* start work on those duties;
b) and at least once every 12 months thereafter.[4]

TDIF Req: FRAUD-02-03-03; **Updated**: Mar-22; **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-02-03-04; **Updated**: Mar-22; **Applicability**: A, C, I
If the *Applicant* is aware of a *Digital Identity Fraud Incident* or *Digital Identity Fraud Risk* which may affect *Users*, the *Applicant* MUST:

a) provide advice to *Users* on how to avoid such incidents or risks; or
b) if *Users* do not interact directly with the *Applicant* or the *Applicant's Identity System,* take reasonable steps to support the provision of such advice by another *Accredited Provider or Relying Party*.

2.4 Fraud monitoring and detection

TDIF Req: FRAUD-02-04-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST implement and maintain a *Digital Identity Fraud* control mechanism to detect actual or suspected *Digital Identity Fraud Incidents.*

TDIF Req: FRAUD-02-04-01a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST implement and maintain a process for *Personnel, Individuals*, *Enforcement Bodies* and other entities to report suspected *Digital Identity Fraud* confidentially.

4 A copy of the training materials will be requested by the DTA as part of initial accreditation and annually thereafter as part of the *Annual Assessment* under *TDIF: 07-Annual Assessment*.

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

The *Applicant* *MUST* implement and maintain a *Digital Identity Fraud* control mechanism to flag actual or suspected *Digital Identity Fraud Incidents*.

TDIF Req: FRAUD-02-04-02a; **Updated**: Mar-22; **Applicability**: A, C, I

The *Applicant* *MUST* compare all new registrations and updates to existing records against the fraud control mechanism used to flag actual or suspected *Digital Identity Fraud Incidents*.

TDIF Req: FRAUD-02-04-02b; **Updated**: Mar-22; **Applicability**: A, C, I

If the *Applicant* reasonably suspects that a *Digital Identity* is fraudulent or its use may result in a *Digital Identity Fraud Incident*, the *Applicant*:

a) *MUST NOT* allow a new registration or update of that *Digital Identity* to be completed; and
b) *MUST* block the use of the *Digital Identity* on its *Identity System*.

2.5 Incident management, investigations and reporting

TDIF Req: FRAUD-02-05-01; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* either:

a) investigate actual and suspected *Digital Identity Fraud Incidents,* unless the incident or suspected incident has been referred to, and been accepted by, an *Enforcement Body*; or
b) if the *Digital Identity Information* held by the *Applicant* in connection with the services for which it is accredited does not include *Personal Information,* take reasonable steps to support an investigation being conducted by another *Entity.*

TDIF Req: FRAUD-02-05-01a; **Updated**: Mar-22; **Applicability**: A, C, I, X

In the event of a *Digital Identity Fraud Incident,* the *Applicant* *MUST* take reasonable steps to:

a) mitigate the adverse effects of the incident; and

b) eliminate or, if it cannot be eliminated, minimise, the risk of recurrence of similar incidents.

TDIF Req: FRAUD-02-05-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST maintain documented procedures setting out criteria for *Digital Identity Fraud Incident* investigation processes and procedures including appropriate criteria for making timely decisions at critical stages in managing a *Digital Identity Fraud Incident*.

TDIF Req: FRAUD-02-05-03; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST keep records of:

a) decisions to use civil, administrative or disciplinary procedures, or to take no further action in response to a *suspected Digital Identity Fraud Incident*; and
b) the Applicant's investigation of and responses to actual and suspected *Digital Identity Fraud Incidents.*

TDIF Req: FRAUD-02-05-04; **Updated**: Mar-22; **Applicability**: A, C, I, X
Where an *Enforcement Body* declines a referral, the *Applicant* MUST resolve the matter in accordance with relevant internal and external requirements.

TDIF Req: FRAUD-02-05-05; **Updated**: Mar-20; **Applicability**: A, C, I, X
The Applicant MUST demonstrate that the *Personnel,* or any external investigators, engaged to conduct *Fraud* investigations are appropriately qualified *Personnel* with relevant qualifications or training to effectively carry out their duties.

TDIF Req: FRAUD-02-05-06; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST:

a) provide the DTA with a report on *Digital Identity Fraud Incidents* at least once every quarter; or
b) if the *Digital Identity Information* held by the *Applicant* in connection with the services for which it is accredited does not include *Personal*

Information, take reasonable steps to support the reporting of *Digital Identity Fraud Incidents* by another *Accredited Provider or Relying Party*.

TDIF Req: FRAUD-02-05-06a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* include, at a minimum, the following information when reporting on *Digital Identity Fraud Incidents*:

a) the number of *Digital Identity Fraud Incidents* related to the *Applicant* in the period since the last report. The number of such incidents may be zero;
b) a description of the type or types of *Digital Identity Fraud Incidents* and their severity; and
c) a description of the measures taken by the *Applicant* in response to the incidents covered by the report.

Depending on the nature of the *Digital Identity Fraud Incident* and legal advice obtained, the *DTA* may advise impacted stakeholders of the outcome of a *Digital Identity* fraud investigation.

2.6 Support for victims of Digital Identity fraud

TDIF Req: FRAUD-02-06-01; **Updated**: Mar-22; **Applicability**: A, C, I
The *Applicant* *MUST* implement a process which allows any *Individual* to notify the *Applicant* when *they* suspect or become aware that they have been affected by a *Digital Identity Fraud Incident*.

TDIF Req: FRAUD-02-06-02; **Updated**: Mar-22; **Applicability**: A, C, I
The *Applicant* *MUST* provide (either directly or through a third party) support services to any *Individuals* who are impacted by a *Digital Identity Fraud Incident.*

TDIF Req: FRAUD-02-06-03; **Updated**: Mar-22; **Applicability**: A, C, I
If the use of a *Digital Identity* has been blocked by the *Applicant* in accordance with FRAUD-02-04-02b, the *Applicant* *MUST* ensure that the *Digital Identity* is not used on the *Applicant's Identity System* unless the *Digital Identity* has been reproofed to the highest *Identity Proofing Level* as applied to the *Digital Identity* before the incident.

3 Privacy Requirements

Applicants for *TDIF Accreditation* should be aware that the TDIF may prescribe a different scope of information handling requirements than those in the *Privacy Act 1988* (Cth). This is to support the TDIF Principles outlined in *TDIF 02 Overview*.

3.1 General privacy requirements

TDIF Req: PRIV-03-01-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The Applicant ***MUST*** comply with applicable laws in relation to the protection and privacy of *Personal Information* including, where relevant, applicable obligations under the *Privacy Act*, including the *Australian Privacy Principles* (*APPs*), *Australian Government Agencies Privacy Code* and relevant, state or territory privacy legislation.

TDIF Req: PRIV-03-01-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
If the *Applicant* is not an *APP Entity*, the *Applicant* ***MUST NOT*** take any action or engage in a practice with respect to *Personal Information* when providing services using its *Identity System* unless:

a) the *Privacy Act* applies to that action or practice as if the *Applicant* were an organisation within the meaning of that Act; or
b) a law of a State or Territory that provides for all of the following applies to the *Applicant* in relation to the action or practice:
   (i) protection of *Personal Information* (including requirements relating to the notification of *Data Breach*es) comparable to that provided by the *Privacy Act* and the *APPs*; and
   (ii) monitoring of compliance with the law; and
   (iii) a means for an *Individual* to seek recourse if the *Individual's Personal Information* is dealt with in a way contrary to the law; or

neither (a) nor (b) apply and the *Applicant* has entered an agreement with the DTA, and the agreement requires the *Applicant* to comply with the *Privacy Act* and the *APPs* in relation to that action or practice as if the *Applicant* were an *APP Entity*.

3.2 Privacy governance

3.2.1 Privacy roles

TDIF Req: PRIV-03-02-01; **Updated**: Mar-22; **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 and ensure that position is held by a person with relevant qualifications and experience to effectively carry out the functions specified for the *Privacy Officer* in PRIV-03-02-01a.

TDIF Req: PRIV-03-02-01a; **Updated**: Mar-22; **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) Handling requests for access to and correction of *Personal information*
c) Maintaining a record of *Personal information* holdings including:
    (i) the types of *Personal Information* collected, held or disclosed;
    (ii) the manner in which such information is received by the *Applicant*; and
    (iii) where such information is held
d) Assisting with the preparation of *Privacy Impact Assessments* (*PIAs*)
e) Maintaining a register of *PIAs*
f) Reviewing and, where relevant, updating the *Privacy Policy* at least annually in accordance with PRIV-03-02-05.

TDIF Req: PRIV-03-02-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* have at least one designated *Privacy Champion* and ensure that position is held by a person with relevant qualifications and experience to effectively carry out the functions specified for the *Privacy Champion* in PRIV-03-02-02a and PRIV-03-02-02b.

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-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* demonstrate how its *Privacy Champion*:

a) approves its *Privacy Management Plan*;
b) reviews the Applicant's progress against the *Privacy Management Plan* as described in PRIV-03-02-07;
c) provides regular reports to the *Applicant's* executive on privacy issues; and
d) provides leadership within the *Applicant* on broader strategic privacy issues.

3.2.2 Privacy Policy

TDIF Req: PRIV-03-02-03; **Updated**: Mar-22; **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 *Applicant*.

TDIF Req: PRIV-03-02-03a; **Updated**: Mar-22; **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-22; **Applicability**: A, I, X

Where an *Applicant* is applying to, or has been, accredited in two or more of the following *Accredited Roles*:

a) an *Identity Service Provider*;
b) an *Attribute Service Provider*;
c) an *Identity Exchange*;

the Applicant *MUST* clearly distinguish between the privacy policy or privacy policies for each *Accredited Role*.[5]

5 This will result in either a separate privacy policy for the Identity Facility for each kind of Accredited Role (i.e., 2 or 3 privacy policies) or a single privacy policy with distinct sections addressing the Applicant's Identity Facility for each kind of Accredited Role.

TDIF Req: PRIV-03-02-04; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant's Privacy Policy* ***MUST*** include information on:

a) The kinds of *Personal information* that the *Applicant* collects and holds.
b) How the *Applicant* 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-22; **Applicability**: A, C, I, X

The *Applicant's Privacy Officer* ***MUST*** review the *Privacy Policy* which covers the *Applicant's Identity System* at least annually and ensure that the *Privacy Policy* is updated where required promptly following such review.

3.2.3 Privacy Management Plan

TDIF Req: PRIV-03-02-06; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant's Privacy Officer* ***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-22; **Applicability**: A, C, I, X

The *Applicant's Privacy Champion* ***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-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* provide appropriate privacy awareness training to *Personnel* whose duties relate to the *Applicant's Identity System*:

a) before such *Personnel* start work on those duties; and
b) at least once every 12 months thereafter.[6]

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*, TDIF privacy requirements, and any relevant privacy laws.

3.3 Privacy Impact Assessment

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

TDIF Req: PRIV-03-03-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* conduct a *Privacy Impact Assessment* on all *High Risk Projects* related to its *Identity System.*

TDIF Req: PRIV-03-03-01a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* maintain a register of the *PIAs* it conducts in respect of its *Identity System*, including *PIAs* referred to in PRIV-03-03-01 and *PIAs* conducted as part of *Functional Assessments.*

TDIF Req: PRIV-03-03-01b; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* publish the register of *PIAs*, or a version of the register, on its website.

6 A copy of the training materials will be requested by the DTA as part of initial accreditation and annually thereafter as part of the *Annual Assessment* under *TDIF: 07-Annual Assessment*.

3.4 *Data Breach* Response Management

TDIF Req: PRIV-03-04-01; **Updated**: Mar-22; **Applicability**: A, C, I, X

If the *Applicant* is an *APP Entity,* the *Applicant* MUST:

a) report eligible *Data Breach*es to affected *Individuals* and the *Information Commissioner* as required under the *Privacy Act*[7]; and

b) if required to notify the *Information Commissioner*—provide the DTA with a copy of the report at the same time it is provided to the *Information Commissioner*.

TDIF Req: PRIV-03-04-01a; **Updated**: Mar-22; **Applicability**: A, C, I, X

If the *Applicant* is not an *APP Entity,* the *Applicant* MUST:

a) if the *Applicant* is a department or authority of a State or Territory and the *Applicant* is covered by a law of State or Territory that provides a scheme for notification of *Data Breach*es that is comparable to the scheme provided for in Part IIIC of the *Privacy Act*, the *Applicant* MUST:

   i. comply with its notification obligations under the relevant State or Territory Scheme; and

   ii. if required to notify another entity—provide the DTA with a copy of any statement provided to the notified entity under such scheme at the same time as it is provided to the notified entity; or

b) if paragraph (a) does not apply to the *Applicant,* the *Applicant* MUST comply with PRIV-03-04-01 as if the *Applicant* were an *APP Entity*.

TDIF Req: PRIV-03-04-02; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* MUST develop and maintain a *Data Breach Response Plan* that:

a) includes a description of the actions to be taken if a *Data Breach* is suspected, discovered, or reported by *Personnel* or external party;

b) lists the roles and responsibilities of *Personnel* involved in managing a *Data Breach*; and

c) includes a clear communication plan and information about when a *Data Breach* is to be:

7 See Part IIIC of https://www.legislation.gov.au/Details/C2019C00025 for the definition of an eligible *Data Breach* including exceptions to reporting.

i. escalated to the *Data Breach* response team;
ii. notified to Individuals affected by the *Data Breach*; and
iii. notified to a third party, including notifications required by law and notifications under PRIV-03-04-01a.

TDIF Req: PRIV-03-04-03; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Data Breach Response Plan* MUST NOT be inconsistent with the *Applicant's Digital Identity Fraud Control Plan* or *System Security Plan.*

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.

TDIF Req: PRIV-03-05-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST notify *Individuals* that the *Applicant* may use the *Individual's* information to detect, manage and investigate *Digital Identity Fraud Incidents*.

3.6 Collection and use limitation

TDIF Req: PRIV-03-06-01; **Updated**: Mar-22; **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 the *Applicant* to provide the services for which it is seeking accreditation.

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-22; **Applicability**: A, C, I, X
The *Applicant* MUST NOT use or disclose *Personal information* for direct marketing purposes, including:

a) offering to supply goods or services;

b) advertising or promoting goods or services;
c) enabling another *Entity* to offer to supply goods or services;
d) enabling another *Entity* to advertise or promote goods or services; or
e) market research.

This requirement does not apply to the disclosure of *Personal Information* if:

f) the information is disclosed for the purposes of offering to supply services or advertising or promoting services that the *Applicant* is seeking accreditation to provide to an *Individual*; and
g) the individual about whom the information is disclosed has expressly consented to the disclosure and receiving communications for purposes permitted by paragraph (f)

TDIF Req: PRIV-03-06-04a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST NOT* use or disclose *Personal information* for enforcement related activities conducted by, or on behalf of, an *Enforcement Body* unless:

a) the *Applicant* is satisfied that the enforcement body reasonably suspects that a person has committed an offence against a law of the Commonwealth or of a State or Territory that is punishable on conviction by imprisonment for at least 3 years or started proceedings against a person for such an offence; or
b) the *Applicant* is satisfied that the enforcement body reasonably suspects that a person has breached a law imposing a penalty of 180 penalty units or more (for an individual) or 900 penalty units or more (for a body corporate), or has started proceedings against a person in relation to the breach; or
c) the information is used or disclosed under a warrant issued by a magistrate, judge or member of a tribunal; or
d) the use or disclosure is otherwise required by a law or *TDIF Requirement* that applies to and is binding on the *Applicant*.

TDIF Req: PRIV-03-06-05; **Updated**: Mar-22; **Applicability**: X
The *Applicant* *MUST* publish in an open and accessible manner an *Annual Transparency Report.*

TDIF Req: PRIV-03-06-05a; **Updated**: Mar-22; **Applicability**: X
Unless prohibited by law, the *Annual Transparency Report* *MUST* disclose:

a) the name of each *Enforcement Body* that has requested *Digital Identity Information* from the *Applicant* since the previous report;
b) the total number of such requests received by the *Applicant*;
c) details of the type or kind of *Digital Identity Information* requested by each *Enforcement Body* (but not so as to include the *Personal Information* of an *Individual*); and
d) the total number of requests that resulted in the *Applicant* providing *Digital Identity Information* in response to the request.

TDIF Req: PRIV-03-06-06; **Updated**: Mar-22; **Applicability**: X
The *Applicant* *MUST NOT* retain *Users' Attributes* or *Restricted Attributes* once they are passed from an *Identity Service Provider* to a *Relying Party* with the exception of:

a) securely storing the *Attributes* for the duration of an authenticated session.
b) *Identity System Metadata* listed in table 2 of the *TDIF 05 Role Requirements*.

3.7 Limitation on use of behavioural information

TDIF Req: PRIV-03-07-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* only collect, use and disclose an *Individual's Behavioural Information* to:

a) provide the services for which the *Applicant* is seeking accreditation;
b) comply with a requirement or authorisation under a law of the Commonwealth, a state or territory;
c) support *Digital Identity* fraud management functions; or
d) improve the performance or usability of the *Applicant's Identity System*.

TDIF Req: PRIV-03-07-01a; **Updated**: Oct-21; **Applicability**: A, C, I, X
The *Applicant* *MUST NOT* sell an *Individual's Behavioural Information* to a third party.

3.8 Collection, Use and Disclosure of biometrics

TDIF Req: PRIV-03-08-01; **Updated**: Mar-22; **Applicability**: C, I
The *Applicant* MUST ensure *Express Consent* is obtained from an *Individual* prior to collecting, using, or disclosing that *Individual's Biometric Information*.

TDIF Req: PRIV-03-08-01a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST NOT collect, use, or disclose an *Individual's Biometric Information* unless:

a) The *Applicant* is seeking accreditation, or is accredited, as an *Identity Service Provider or Credential Service Provider* and the *Biometric Information* is being collected, used or disclosed for the purposes of conducting *Biometric Binding* as part of an *Identity Proofing Process* or authenticating the *Individual* to their *Digital Identity;* or
b) The *Biometric Information* is being collected, used or disclosed for the purposes of creating a government issued *Identity document*.

TDIF Req: PRIV-03-08-02; **Updated**: Mar-22; **Applicability**: C, I
Subject to PRIV-03-08-02a, *Biometric information* MUST be destroyed:

a) if collected by an *Identity Service Provider* for the purpose of conducting *Biometric Binding* as part of an *Identity Proofing Process*, immediately after the *Biometric Binding* process is complete; or
b) if collected by a *Credential Service Provider* with the *Express Consent* of an *Individual* for the purpose of authenticating that *Individual* to their *Digital Identity*, immediately after the consent is withdrawn.

TDIF Req: PRIV-03-08-02a; **Updated**: Mar-22; **Applicability**: A, C, I
In accordance with PRIV-03-08-02, the *Applicant MUST* destroy *Biometric information* unless the *Biometric information* is collected or was collected to create a government issued *Identity document* and the *Applicant* is an *Identity Document Issuer* for that *Identity Document* [8]

[8] For example where a *Road Traffic and Transport Authority* is an *Identity document issuer* and an *Identity Service Provider*.

TDIF Req: PRIV-03-08-02b; **Updated:** Mar-22; **Applicability:** C, I
When destroying or retaining *Biometric Information* in accordance with PRIV-03-08-02, the *Applicant MUST* ensure that it is responsible for the destruction or retention of all collected *Biometric Information*, including all copies, caches, and intermediary databases, including any subcontracted or third-party components. The Applicant *MUST* provide evidence of this to the DTA.

TDIF Req: PRIV-03-08-02c; **Updated:** Mar-22; **Applicability:** C, I
When destroying *Biometric Information*, the *Applicant MUST* create and maintain a record that the destruction of *Biometric Information* has occurred.[9]

TDIF Req: PRIV-03-08-03; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant MUST NOT* use a *Biometric Matching* algorithm to perform *one-to-many matching*.[10]

TDIF Req: PRIV-03-08-04; **Updated**: Mar-22; **Applicability**: C, I
If the *Applicant* can collect, use or disclose *Biometric Information* under PRIV-03-08-01a, the *Applicant MAY* disclose that biometric information to the *Individual* to whom the information relates.

3.9 Express Consent

TDIF Req: PRIV-03-09-01; **Updated:** Mar-22; **Applicability**: A[11], C, I[12], X[13]
The *Applicant MUST* ensure *Express Consent* is obtained from an *Individual* prior to disclosing that *Individual's Attributes* to a *Relying Party* or any third party (including an *Authoritative Source)*.

9 This evidence can be documented by an Audit Log in accordance with PROT-04-02-22a.

10 This includes collecting, using, or disclosing an *Individual's Biometric Information* for the purposes of Identifying an individual and using the biometric to determine whether the individual has multiple digital identities.

11 If the *Attribute 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 *Attribute Service Provider*.

12 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*.

13 If the connection to the *Relying Party* is brokered by an *Identity Exchange*, the *Identity Exchange* may delegate the collection of *Express Consent* to the *Identity Service Provider or Attribute Service Provider*.

TDIF Req: PRIV-03-09-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
If the *Applicant* is obtaining enduring *Express Consent* from a *User,* they *MUST* implement the following requirements: (PRIV-03-09-02a, PRIV-03-09-02b, PRIV-03-09-02c 02a, and PRIV-03-09-02d) for the operation of withdrawal of enduring *Express Consent*.

TDIF Req: PRIV-03-09-02a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant MUST* allow an *Individual* to withdraw or vary their *Express Consent*.

TDIF Req: PRIV-03-09-02b; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant MUST* demonstrate how this *Express Consent* withdrawal or variation process is straightforward and easy to use.

TDIF Req: PRIV-03-09-02c; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant MUST* include a clear description of the process to withdraw or vary the *Express Consent* in the *Applicant's Privacy Policy*.

TDIF Req: PRIV-03-09-02d; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant MUST,* at the time of obtaining enduring consent, notify *Individuals*:

a) that providing enduring *Express Consent* is optional;
b) of the implications of providing or not providing their enduring *Express Consent*; and
c) of the process for withdrawing or varying their enduring *Express Consent*.

TDIF Req: PRIV-03-09-03; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant MUST* maintain *Audit Logs* that demonstrate how *Express Consent* was obtained from the *Individual*, including:

a) the date and method by which *Express Consent* was obtained from the *Individual*;
b) the duration of the *Express Consent*;
c) the terms of the *Express Consent*; and
d) whether the *Express Consent* has been withdrawn or has expired.

TDIF Req: PRIV-03-09-04; **Updated**: Mar-22; **Applicability**: A, I
The *Applicant* *MUST* inform *Individuals* of other channels available to verify their *Identity* and make clear to the *Individual* what the consequences are of declining to provide *Express Consent* or the required information.

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**: Jun-21; **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 *DTA's* reasonable satisfaction it has appropriate contractual and practical measures to ensure the overseas recipient complies with these *TDIF* privacy requirements.

3.11 Single Identifiers

TDIF Req: PRIV-03-11-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST NOT* create and assign a unique *identifier* to a *User* for use across an *Identity Federation*.

3.12 Access and correction

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-22; **Applicability**: A, C, I
The *Applicant* *MUST* provide *Individuals* with clear instructions on how to update their *Personal information.*

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*)[14] and *Australian Government Information Security Manual* (*ISM*)[15] 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* or *ISM* are to be interpreted as references to the *Applicant*.
- References to *PSPF*, or *ISM* controls that are applicable to an agency are to be interpreted as being applicable to the *Applicant*.
- The scope of *PSPF*, 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 sensitivity and security classification of information.

To the extent of 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.

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.

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

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

- Sound security planning.
- Investigation and response.
- Assurance and review processes.
  Proportionate reporting.

4.1.1 General

TDIF Req: PROT-04-01-01; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* conduct an assessment of the *Cyber Security Risks* in relation to the *Applicant* prior to accreditation and at least once every 12 months beginning on the date the *Applicant* is accredited.

TDIF Req: PROT-04-01-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST*:

a) Determine and record the *Applicant's* tolerance for *Cyber Security Risks*.
b) Manage the *Applicant's Cyber Security Risks*, including by complying with the requirements of this section.
c) Demonstrate how its protective security controls (including controls for *Cyber Security Risks*) are applied to its *Identity System*.
d) Consider the implications their risk management decisions have for *Accredited Providers, Relying Parties and Users* and share information on risks with them where appropriate.

TDIF Req: PROT-04-01-03; **Updated**: Mar-22; **Applicability**: A, C, I, X
Where exceptional circumstances prevent or affect the *Applicant's* capability to implement a TDIF requirement, the *Applicant*:

- *MUST,* as soon as practicable notify the DTA of the circumstances and the non-compliance, including details of the remedial action (if any) taken or to be taken to reduce the risk to the *Applicant's Identity System.*
- *MUST* keep a record of decisions taken by the *Applicant* in relation to such non-compliance and remedial action (if any). These decisions will be requested by the *DTA* during *Annual Assessments*.
- *MAY* vary the *Applicant's* protective security arrangements (including, if relevant, the *System Security Plan*), for a limited period of time, but not so

as to increase the level of *Cyber Security Risk* above the *Applicant's* risk tolerance.

4.1.2 Management structures and responsibilities

TDIF Req: PROT-04-01-04; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* have an officer or senior employee of the *Applicant* as the designated *Chief Security Officer* (CSO) or equivalent role who is responsible for:

a) managing *Cyber Security Risks* within their organisation; and
b) ensuring the *Applicant* complies with the protective security requirements in this section.

TDIF Req: PROT-04-01-04a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* empower the *CSO* or equivalent role to make and implement decisions about:

a) Appointing security advisors within the *Applicant's* organisation to support the CSO in the day-to-day delivery of protective security services.
b) The *Applicant's* protective security planning.
c) The *Applicant's* protective security practices and procedures.
d) Investigating, responding to and reporting on *Cyber Security Incidents*.

TDIF Req: PROT-04-01-05; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* ensure *Personnel* are aware of their collective responsibility to foster a positive security culture.

TDIF Req: PROT-04-01-05a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* provide appropriate information and training in relation to the prevention and management of *Cyber Security Risks* to *Personnel* whose duties relate to the services for which the *Applicant* is accredited*:*

a) before such *Personnel* start work on those duties; and
b) at least once in every 12 months thereafter.[16]

16 A copy of the training materials will be requested by the DTA as part of initial accreditation and annually thereafter as part of the *Annual Assessment* under *TDIF: 07-Annual Assessment*.

TDIF Req: PROT-04-01-06; **Updated**: Jun-21; **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 *DTA*.
c) Relevant security policy or legislative obligations are met.

TDIF Req: PROT-04-01-07; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* maintain records of instructions it gives its *Personnel* and contractors and its procedures to assist *Personnel* and contractors to prevent, detect, report and deal with *Cyber Security Risks*.

TDIF Req: PROT-04-01-08; **Updated**: Mar-22; **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-04-01-09; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST:*

a) maintain a monitored central communications channel (such as an email address) for all security-related matters across governance, *Personnel*, information, *ICT* and physical security, including in relation to *Cyber Security Risks* related to the *Applicant*; and
b) ensure *Personnel* are aware of the communications channel and the purposes for which it is to be used.

TDIF Req: PROT-04-01-10; **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 System security plan

TDIF Req: PROT-04-01-11; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* have in place a *System Security Plan* approved by the *CSO* to manage the *Applicant's Cyber Security Risks*.[17]

TDIF Req: PROT-04-01-11a; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *System Security Plan* *MUST* include:

a) The Cyber security goals and strategic objectives of the *Applicant*, including how *Cyber Security Risk* management intersects with and supports broader business objectives and priorities.
b) The *Applicant's* strategies to implement *Cyber Security Risk* management and maintain a positive *Cyber Security Risk* culture.
c) The *Applicant's* tolerance of *Cyber Security Risks*.
d) The *Personnel*, information, ICT and assets that are critical to the ongoing operation of the Applicant's *Identity System.*
e) The maturity of the *Applicant's* capability to manage *Cyber Security Risks* and the proposed steps to enhance that capability or meet new or emerging risks, threats or vulnerabilities.
f) A summary of the threats, risks and vulnerabilities that impact the confidentiality, integrity and availability of the *Applicant's Identity System*.
g) An assessment of the significance of the threats, risks, and vulnerabilities in paragraph (f).
h) The treatment strategies and controls put in place to manage *Cyber Security Risks* and vulnerabilities.
i) The strategies to ensure the *Applicant* meets its training and awareness needs in relation to the prevention and management of *Cyber Security Risks.*
j) Details of the training that will be provided under paragraph (i);
k) The procedures and mechanisms for *Cyber Security Incident* management, cyber security investigations and reporting *Cyber Security Incidents.*
l) An outline of key roles and responsibilities for protective security control within the *Applicant's* organisation including one or more risk steward/s (or manager/s) who are responsible for each *Cyber security risk* or category of *Cyber security risk*, including for shared risks.

[17] An Applicant's *System Security Plan* may be a component of an overall system security plan for the Applicant.

m) Flexible measures that can be implemented where necessary to meet variations in threat levels, including changes in the national terrorism threat level.
n) The risk ratings and scale to be used by the *Applicant* when assessing the severity of a *Cyber Security Incident*.
o) Where applicable, a description of the location(s) from which *Local Biometric Binding* will be undertaken by the *Applicant*.

TDIF Req: PROT-04-01-12; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant MUST* review and update its *System Security Plan:*

a) at least annually; and
b) as soon as practicable after:
    i. the Applicant becomes aware of a *Cyber Security Incident* in connection with its *Identity System* which is of a type not covered in the *System Security Plan* or which exceeds the *Applicant's* recorded tolerance for *Cyber Security Risks*;
    ii. the *Applicant* becomes aware of a breach of the requirements of its *System Security Plan*; or
    iii. a change in the structure, functions or activities of the *Applicant* (including a change to the *Applicant's Identity System*) where such change may increase their level of *Cyber Security Risk*.

TDIF Req: PROT-04-01-13; **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.

4.1.4 Security maturity monitoring

TDIF Req: PROT-04-01-15; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST assess the maturity of its capability to manage *Cyber Security Risks* and risk culture by considering its progress against goals and strategic objectives identified in its *System Security Plan*.

TDIF Req: PROT-04-01-15a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST document and present evidence to the *DTA* of the maturity of the Applicant's capability to manage *Cyber Security Risks*.

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

TDIF Req: PROT-04-02-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST:

a) Identify *Digital Identity Information* in the possession or control of the *Applicant*.
b) Assess the sensitivity of such information and the importance of the information to the *Applicant's Identity System*.
c) Implement appropriate controls to secure such information against loss, interference, misuse, unauthorised access, unauthorised modification or unauthorised disclosure.[18]

TDIF Req: PROT-04-02-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST ensure information it holds is stored, transferred, transmitted and disposed of securely. This includes ensuring *Sensitive information* (within the meaning of that term in PSPF 08) is appropriately destroyed or archived when it

[18] Some or all of the functions listed in PROT-04-02-01 may also be carried out by the *Applicant's Privacy Officer*.

has passed minimum retention requirements or reaches authorised destruction dates.

4.2.2 Access to information

TDIF Req: PROT-04-02-03; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* ***MUST*** enable appropriate access to *Digital Identity Information*. This includes:

a) Ensuring that access to *Sensitive information*, *Digital Identity Information* or components of the *Identity System* on which such information is stored is only provided to people with a *Need to know* that information.
b) Controlling access (including remove access) to supporting ICT systems, networks, infrastructure, devices and applications used by the *Applicant* in connection with its *Identity System*.

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 identification, authentication and authorisation practices on each occasion where system access is granted.

TDIF Req: PROT-04-02-04a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The Applicant ***MUST*** record each occasion where access is authorised, denied, limited or removed in accordance with PROT-04-02-04, and the identity of the *Individual* on each such occasion.

4.2.3 Safeguarding information from cyber threats

TDIF Req: PROT-04-02-05; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* ***MUST*** mitigate common and emerging cyber threats, including, at a minimum, by implementing and maintaining controls for:

a) application control
b) patching applications
c) restricting administrative privileges; and
d) patching operating systems

as described in the *ASD Strategies to Mitigate Cyber Security Incidents.*[19]

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

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

4.2.4 Incident management, investigations and reporting

TDIF Req: PROT-04-02-07; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* implement and maintain a mechanism for detecting *Cyber Security Incidents* and suspected *Cyber Security Incidents* which occur in connection with its *Identity System.*

TDIF Req: PROT-04-02-07a; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* implement and maintain a process for *Personnel, Individuals, Enforcement Bodies* and other entities to report suspected *Cyber Security Incidents* confidentially.

TDIF Req: PROT-04-02-08; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* implement and maintain a control mechanism to flag *Cyber Security Incidents* or suspected *Cyber Security Incidents* which occur in connection with its *Identity System.*

TDIF Req: PROT-04-02-08a; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* compare all new registrations and updates to existing records against the control mechanism used to flag actual or suspected *Cyber Security Incidents*.

TDIF Req: PROT-04-02-08b; **Updated**: Mar-22; **Applicability**: A, C, I

If the *Applicant* reasonably suspects that the registration or update of a *Digital Identity* is likely to create a *Cyber Security Incident*, the *Applicant*:

a) *MUST NOT* allow a new registration or update *of that Digital Identity* to be completed; and

[19] In addition, the DTA recommends that the *Applicant* implement the essential eight as set out in the *ASD Strategies to Mitigate Cyber Security Incidents*

b) *MUST* block the use of the *Digital Identity* on its *Identity System.*

TDIF Req: PROT-04-02-09; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant MUST* maintain documented procedures setting out criteria for *Cyber Security Incident* investigation processes and procedures including appropriate criteria for making timely decisions at critical stages in managing a *Cyber Security Incident.*

TDIF Req: PROT-04-02-10; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant MUST* take responsibility for investigating actual or suspected *Cyber Security Incidents* which occur in connection with its *Identity System*, including investigating disciplinary matters, unless the matter is referred to and accepted by the Australian Cyber Security Centre or an *Enforcement Body*.

TDIF Req: PROT-04-02-11; **Updated**: Mar-20; **Applicability**: A, C, I, X
Where an *Enforcement Body* 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* demonstrate that the *Personnel,* or any external investigators, engaged to conduct security investigations are appropriately qualified *Personnel* with relevant qualifications or training to effectively carry out their duties.

TDIF Req: PROT-04-02-13; **Updated**: Mar-22; **Applicability**: A, C, I, X
In the event of a *Cyber Security Incident* which impacts the *Applicants Identity System,* the *Applicant MUST* take reasonable steps to:

a) mitigate the adverse effects of the incident; and
b) eliminate or, if it cannot be eliminated, minimise, the risk of recurrence of similar incidents.

TDIF Req: PROT-04-02-14; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant MUST* report *Cyber Security Incidents* which occur in connection with their *Identity System* to the *DTA* at least once every quarter.

TDIF Req: PROT-04-02-14a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* include the following information when reporting *Cyber Security Incidents*:

a) the number of *Cyber Security Incidents* which occurred in connection with the *Applicant's Identity System* in the period since the last report. The number of such incidents may be zero
b) a description of the type or types of *Cyber Security Incidents* and their severity; and
c) a description of the measures taken by the Applicant in response to the incidents covered by the report.

4.2.5 Support for victims of security incidents

TDIF Req: PROT-04-02-15; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* implement a process which allows *Individuals* to notify them when they suspect or become aware of a *Cyber Security Incident*.

TDIF Req: PROT-04-02-16; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* provide (either directly or through a third party) support services to *Individuals* who are impacted by *Cyber security incidents* which occur in connection with the *Applicant's Identity System*.

TDIF Req: PROT-04-02-17; **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-04-02-18; **Updated**: Mar-22; **Applicability**: A, C, I
If the use of a *Digital Identity* has been blocked by the *Applicant* in accordance with PROT-04-02-08b as a result of a *Cyber Security Incident*, the *Applicant* *MUST* ensure that the *Digital Identity* is not used on the *Applicant's Identity System* unless the *Digital Identity* has been reproofed to at least the *same Identity Proofing Level* that applied to the *Digital Identity* before the incident.

4.2.6 Robust ICT systems

TDIF Req: PROT-04-02-19; **Updated**: Mar-22; **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-04-02-20; **Updated**: Mar-22; **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 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-04-02-21; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST NOT* process, store or communicate *Sensitive information* (within the meaning of that term in PSPF 08) on its *Identity System*, unless the residual *Cyber Security Risks* to the *Identity System* and *Digital Identity Information* have been recognised and accepted by the *CSO* or a security advisor on behalf of the *CSO*.

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

The *Applicant* *MUST* ensure their *ICT* systems (including software) incorporate processes for generating *Audit Logs*.

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

At a minimum, *Audit Logs* *MUST* record 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
- for an *Identity Service Provider*, the binding of *Attributes* to a *Digital Identity*; and

- for an *Attribute Service Provider*:
    - the binding of *Attributes* to a *Digital Identity*; and
    - the retrieval of *Attributes* by a third party.

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

At a minimum, *Audit Logs* ***MUST*** include[20] the following details for each event:

- The date and time
- The relevant *User*, identifier or process. Each activity must have a unique identifier
- The description
- The *ICT* equipment involved
- 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*; and
- A unique identifier for the device being used in the event (such as an *International Mobile Equipment Identity* (*IMEI*) of a mobile phone if a mobile phone is used to *Authenticate* to the *Identity System*)

TDIF Req: PROT-04-02-22c; **Updated**: Mar-22; **Applicability**: C

Audit logs ***MUST*** include for each event:

- *Credential Type* used.
- *Credential Level* achieved.

TDIF Req: PROT-04-02-22d; **Updated**: Mar-22; **Applicability**: I

Audit Logs ***MUST*** include for each event the *Identity Proofing Level* of the *Digital Identity* used, if any.

TDIF Req: PROT-04-02-22e; **Updated**: Mar-22; **Applicability**: X

Audit Logs ***MUST*** include for each event:

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

- Interaction type. (e.g. *OIDC Authentication Request* and response)
- Unique interaction identifier
- The name of the *Identity Service Provider* or a *Relying Party*
- Any unique identifier used in the activity
- Names of any *Attributes* requested and returned; and
- Any *Identity Proofing Level* or *Credential Level* requested and returned.

TDIF Req: PROT-04-02-23; **Updated**: Mar-22; **Applicability**: A, C, I, X

Each *Audit Log* *MUST* be:

- Protected and stored to ensure the accuracy and integrity of data captured or held
- Protected from unauthorised access, modification and deletion; and
- Retained for a minimum of 3 years from the date it was generated.

TDIF Req: PROT-04-02-23a; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Audit Logs* *MUST NOT* contain *Biometric information*.

4.2.7 Disaster recovery and business continuity management

TDIF Req: PROT-04-02-24; **Updated**: Mar-22; **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; and
e) Testing requirements and restoration procedures.

TDIF Req: PROT-04-02-25; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* test their *Disaster Recovery and Business Continuity Plan* as part of initial accreditation and at least once every 12 months thereafter.[21]

21 Evidence of testing of the *Applicant's Disaster Recovery and Business Continuity Plan* will be requested by the DTA as part of initial accreditation and annually thereafter as part of the *Annual Assessment* under *TDIF: 07-Annual Assessment*.

4.2.8 Cryptography

TDIF Req: PROT-04-02-26; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* use:

- *Australian Signals Directorate Approved Cryptographic Algorithms* (*AACAs*); and
- *Australian Signals Directorate Approved Cryptographic Protocols* (*AACPs*),

to protect all *Digital Identity Information* while in transit and at rest.

TDIF Req: PROT-04-02-27; **Updated**: Mar-22; **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) Details of the records that will be generated by the *Applicant* in relation to its use of keys and 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 System*.

TDIF Req: PROT-04-03-02; **Updated**: Mar-22; **Applicability**: A, C, I, X

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

a) *Verifying* the identity of *Personnel*; and
b) Confirming eligibility of such *Personnel* 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-22; **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 and take reasonable steps to mitigate any identified risks.

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 *Cyber 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-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* dispose of physical assets securely, including by:

a) resetting combination locks to factory settings;
b) removing all contents from physical assets and performing a visual inspection to confirm such removal; and
c) sanitising or destroying *ICT*.

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[22] for its *Identity System*.

TDIF Req: UX-05-01-05a; **Updated**: Mar-22; **Applicability**: I

The individual journey map *MUST* address each alternative channel made available to a *User* to complete a specific activity.

22 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 proofing 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-22; **Applicability**: I

The *Applicant* *MUST* provide *Users* with information on:

a) the required *Identity documents*
b) whether each piece is mandatory; and
c) the consequences for not providing the complete set of required documents.[23]

TDIF Req: UX-05-02-04; **Updated**: Mar-22; **Applicability**: I

If a code or number is issued by the *Applicant* to a *User* as part of the identity proofing process, the *Applicant* *MUST* notify the *User* in advance that they will receive a digital code or number, how it will be issued and what to do with it.

23 *Individuals* will need to know the specific combinations of *identity documents* which are required to achieve a given *Identity Proofing Level.* .

TDIF Req: UX-05-02-05; **Updated**: Mar-22; **Applicability**: I

The *Applicant* *MUST* advise the *User* on the outcome of the *Identity Proofing* process.

TDIF Req: UX-05-02-05a; **Updated**: Mar-22; **Applicability**: I

If proofing is successful, the *Applicant* *MUST* send the *User* confirmation regarding the successful completion of *Identity Proofing* and information on next steps.

TDIF Req: UX-05-02-05b; **Updated**: Mar-22; **Applicability**: I

If proofing is partially complete[24], the *Applicant* *MUST* inform the *User* of:

a) information and documents that will be deleted by the *Applicant*
b) information and documents that will be retained by the *Applicant* and the period for which such information and documents will be retained; and
c) further information and documents to be provided by the *User* in order to successfully complete the relevant identity proofing process.

TDIF Req: UX-05-02-05c; **Updated**: Mar-22; **Applicability**: I

If proofing is unsuccessful, the *Applicant* *MUST* provide the *User* with:

a) an option to either:
    i. continue with the proofing process using one or more alternative channels; or
    ii. not continue with the proofing process; and
b) details of the alternative channels under paragraph (a) above and clear instructions on how to use such alternative channels.

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

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

24 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-05-02-07; **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 proofing 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.

5.4 Usability testing

5.4.1 Limited exception for Applicants not interacting with Users

TDIF Req: UX-05-04-01; **Updated:** Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MUST* meet the requirements in Section 5.4.2 (Usability Test Plans) and Section 5.4.3 (Conduct Usability Testing) unless it can demonstrate to the DTA that the *Applicant* has:

1) no interaction with a user when providing the services for which the Applicant is seeking accreditation; or
2) limited interaction with a User when providing the services for which the Applicant is seeking accreditation, including where the User is interacting with the Applicant's Identity System and has:

a. determined, through a risk assessment, that there is a low risk that the failure to conduct the usability testing will adversely impact the usability of the Applicant's Identity System; and
b. taken reasonable steps, including processes and procedures, to:
    i. obtain and record feedback from users about the usability of the Applicant's Identity System; and
    ii. incorporate such feedback into the design of its Identity System.

5.4.2 Usability test plans

TDIF Req: UX-05-04-02; **Updated**: Mar-22; **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-05-04-02a; **Updated**: Mar-22; **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* to participate in the usability testing.

TDIF Req: UX-05-04-02b; **Updated**: Mar-22; **Applicability**: A, C, I, X
The range of representative *Individuals* *MUST* include:

a) *Individuals* with disability.
b) *Individuals over the age of 65*.
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-05-04-02c; **Updated**: Mar-22; **Applicability**: A, C, I, X
The range of representative *Individuals* *MUST* be from a diverse range of gender classifications.

5.4.3 Conduct usability testing

TDIF Req: UX-05-04-03; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* use experienced *User Researchers* to conduct usability testing of its *Identity System* in accordance with its usability test plan. For the purpose of this requirement, an experienced *User Researcher* is one who is highly skilled in identifying individual needs, conducting usability tests, and feeding insights back to the product team.

TDIF Req: UX-05-04-04; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* conduct usability testing on its *Identity System* as part of initial accreditation and at least once every 12 months thereafter. [25]

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

The *Applicant* *MUST* conduct usability testing of its *Identity System* across all relevant components of the *Applicant's Identity System*, in a production-like environment.

TDIF Req: UX-05-04-06; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* ensure that the *User Researcher* prepares a usability testing report that documents the outcomes of its usability testing, including test methodology(s), test results, findings and recommendations.

25 Evidence of testing of the *Applicant's usability testing* will be requested by the DTA as part of initial accreditation and annually thereafter as part of the *Annual Assessment* under *TDIF: 07-Annual Assessment*.

TDIF Req: UX-05-04-06a; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant's Accountable Executive* must respond in writing to any recommendation identified in the usability testing report including:

a) for each recommendation in the report that is accepted by the *Applicant*, the timeframe for implementation of the recommendation; and
b) for each recommendation in the report that is not accepted by the *Applicant*, the reasons for non-acceptance and details of alternative actions (if any) to be taken by the *Applicant*.

TDIF Req: UX-05-04-06b; **Updated**: Mar-22; **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*.

5.5 Accessibility requirements

TDIF Req: UX-05-05-01; **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 supported by the *Applicant's Identity System*.

6 Technical testing requirements

TDIF Req: TEST-06-01-01**; Updated:** Mar-22**; Applicability:** A, C, I, X
For the *Technical Testing* that the *Applicant* is required to complete under this section, it *MUST* provide the DTA with the following:

a) The exit criteria used when testing
b) The assumptions, limitations and dependencies relevant to the testing; and
c) The methodology used to conduct testing, including a description of the data used, and the environment used to conduct testing

TDIF Req: TEST-06-01-02**; Updated:** Mar-22**; Applicability:** A, C, I, X
The *Applicant MUST* develop a *Requirements Traceability Matrix* (RTM) which maps the tests completed to the *TDIF* requirements they are being used to demonstrate compliance with.

TDIF Req: TEST-06-01-03**; Updated:** Mar-22**; Applicability:** A, C, I, X
The *Applicant MUST* provide the DTA with a technical test report detailing the outcomes of the *Technical Testing* done under this section, including:

a) Confirmation that the testing has been undertaken and completed
b) The results of the testing, including any defects detected in testing, and whether these have been addressed; and
c) Evidence that the exit criteria specified for testing has been met.

TDIF Req: TEST-06-01-04**; Updated:** Mar-22**; Applicability:** A, C, I, X
The *Applicant MUST* demonstrate through *Technical Testing* how its *Identity System* meets the following *TDIF* requirements:

- Its fraud control mechanism for detecting *Digital Identity Fraud Incidents* (as per FRAUD-02-04-01).
- Its fraud control mechanism to flag incidents of *Digital Identity Fraud Incidents* (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-04-02-22).
- The activities and events logged (as per PROT-04-02-22a).
- The content included in activity logs (as per PROT-04-02-22b, PROT-04-02-22c, and PROT-04-02-22d and PROT-04-02-22e).

TDIF Req: TEST-06-01-05**; Updated:** Mar-22**; 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-22**; Applicability:** I
The *Applicant* MUST demonstrate through *Technical Testing* the functionality of all verification methods, *Identity Proofing Levels*, identity lifecycle management processes and any *Step-up* processes supported by the *Applicant's Identity System.*

TDIF Req: TEST-06-01-07**; Updated:** Mar-22**; Applicability:** C
The *Applicant* MUST demonstrate through *Technical Testing* the functionality of all *Credential Levels*, *Credentials, Credential* lifecycle management processes and any *Step-Up* processes supported by the *Applicant's Identity System*.

7 Functional Assessments

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

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

7.1 Functional Assessment Requirements

TDIF Req: ASSESS-07-01-01; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* MUST ensure an *Assessor* conducts:

a) a *Privacy Impact Assessment* in accordance with ASSESS-07-05-01
b) a *Privacy Assessment* in accordance with ASSESS-07-05-03
c) a *Penetration Test* in accordance with ASSESS-07-06-02
d) a *Security Assessment* in accordance with ASSESS-07-06-01; and
e) an *Accessibility Assessment* in accordance with ASSESS-07-07-01.

TDIF Req: ASSESS-07-01-02; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* MUST:

a) define and prepare written instructions on the scope[26], objectives and criteria for each *Functional Assessment*
b) ensure such written instructions are consistent with the TDIF requirements
c) provide a copy of such instructions to the relevant *Assessor* prior to commencement of the *Functional Assessment*; and
d) ensure that each *Functional Assessment* is conducted in accordance with such written instructions.

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

7.2 Assessor skills, experience and independence

TDIF Req: ASSESS-07-02-01; **Updated**: Mar-22; **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 relevant *Functional Assessment*.

TDIF Req: ASSESS-07-02-02; **Updated**: Mar-22; **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*.

7.3 Functional Assessment process

TDIF Req: ASSESS-07-03-01; **Updated**: Mar-22; **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-07-03-02; **Updated**: Mar-22; **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-07-03-03; **Updated**: Mar-22; **Applicability**: A, C, I, X
If required by an *Assessor or* the *DTA*, the *Applicant* MUST take reasonable steps to permit the *Assessor* to undertake a site visit to the *Applicant's* premises or other location where it provides services in connection with its *Identity System*.

TDIF Req: ASSESS-07-03-04; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* ensure that each *Assessor* prepares a report on the outcomes of the relevant *Functional Assessment* that includes:

a) test results where applicable
b) an assessment of whether the *Applicant's Identity System* meets the applicable requirements of the *TDIF*
c) recommendations by the *Assessor*; and
d) such other information required by the *Applicant* to enable it to comply with the TDIF and prepare the *Functional Assessment Report*.

7.4 Functional Assessment Report

TDIF Req: ASSESS-07-04-01; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* document the outcomes of each *Functional Assessment* in a *Functional Assessment Report.* The *Applicant's Functional Assessment Report* *MUST* include, for each *Functional Assessment*:

a) A summary of the activities performed by the *Assessor* during the *Functional Assessment*.
b) The dates on which the *Functional Assessment* was commenced and completed.
c) Name, role (or position) and contact details of the relevant *Accountable Executive* and point of contact.
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) The *Assessor's* opinion on whether the *Applicant's Identity System* meets the applicable *TDIF* requirements, including any requirements that could not be adequately assessed due to access or timing issues.

j) Details of any identified instance of non-compliance with the TDIF requirements or any other risk identified by the *Assessor*.
k) Any recommendation from the Assessor to address such non-compliance or risk.

TDIF Req: ASSESS-07-04-02; **Updated:** Mar-22; **Applicability:** A, C, I, X
The *Applicant* *MUST*:

a) Assess each identified instance of non-compliance with the TDIF requirements covered by the *Functional Assessment* report as per ASSESS-07-04-01
b) Assess any other risks identified by the *Assessor*
c) Assign each instance of non-compliance and risk with a risk rating as set out in **Appendix A: Risk Ratings**; and
d) Include in the *Functional Assessment Report:*
    i. Details of each such risk assessment
    ii. A copy of the *Applicant's* risk matrix; and
    iii. Descriptions of the likelihood and risk categories associated with the risk ratings assigned above.

TDIF Req: ASSESS-07-04-03; **Updated:** Mar-22; **Applicability:** A, C, I, X
The *Applicant*'s *Accountable Executive* *MUST* respond in writing to each recommendation, risk and non-compliance outlined in the *Functional Assessment Report* including:

a) for each recommendation, risk and non-compliance that is accepted by the *Applicant*, the timeframe and details of the actions that the *Applicant* will take for implementation[27]; and
b) for each recommendation, risk and non-compliance that is not accepted by the *Applicant*, the reasons for non-acceptance and details of alternative actions (if any) to be taken by the *Applicant*.

[27] Applicants must be aware of their ongoing obligations regarding items on their Forward Work Plan. Detailed information, including requirements and guidance can be found in Section 2.8.1 Forward Work Plan of *TDIF 07 Maintain Accreditation*

TDIF Req: ASSESS-07-04-03a; **Updated**: Mar-22; **Applicability**: A, C, I, X
Any recommendation, risk or non-compliance identified in ASSESS-07-04-03 *MUST NOT* meet or exceed a Moderate, High or Extreme risk rating[28] for the *Applicant's Initial Assessment*.

TDIF Req: ASSESS-07-04-03b; **Updated**: Mar-22; **Applicability**: A, C, I, X
If the risk rating meets or exceeds that outlined above in ASSESS-07-04-03a, the Accredited Provider *MUST* confirm:

- it has implemented mitigations to address the recommendation, risk or non-compliance; and
- The recommendation, risk or non-compliance has been reassessed and the residual risk rating is at Low or Compliant; and
- The *Accountable Executive* has signed off and confirmed the implemented mitigation of the recommendation, risk or non-compliance and the new residual risk rating.

NOTE: Applicants MUST be aware that a Moderate, High or Extreme risk rating is grounds for a failed Initial Assessment and that the DTA will not grant TDIF accreditation until the items required in ASSESS-07-04-03b are complete and the DTA is satisfied that the risk is sufficiently mitigated. **Appendix A: Risk Ratings** in this document contains further details outlining the conditions of each risk rating.

7.5 PIA and Privacy Assessment

TDIF Req: ASSESS-07-05-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant MUST* commission an *Assessor* to conduct a *Privacy Impact Assessment* on their *Identity System* as part of Initial accreditation[29].

TDIF Req: ASSESS-07-05-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Privacy Impact Assessment* conducted under ASSESS-07-05-01 *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*.

[28] According to Appendix A in TDIF 04 Functional Requirements, or the Applicant's equivalent risk framework.
[29] Applicants must be aware that a Privacy Impact Assessment is required to be conducted on any high-risk projects after Initial Accreditation as per PRIV-03-03-01.

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-07-05-03; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST commission an *Assessor* to conduct a *Privacy Assessment* (which is separate to and follows on from the *PIA* under ASSESS-07-05-01) as part of initial accreditation and annually thereafter as part of the *Annual Assessment*. The *Privacy Assessment MUST:*

a) address the recommendations (if any) included in the *Privacy Impact Assessment* under ASSESS-07-05-01; and
b) includes a review and assessment of the *Applicant's* compliance with the privacy requirements of the TDIF.

7.6 Security assessment and penetration test

TDIF Req: ASSESS-07-06-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST commission an *Assessor* to conduct a *Security Assessment* of its *Identity System* to identify security deficiencies as part of initial accreditation and annually thereafter as part of the *Annual Assessment*. The *Security Assessment* must, at a minimum:

a) include a review and assessment of the *Applicant's* compliance with the applicable Protective Security Requirements; and
b) address the findings and recommendations (if any) from the *Penetration testing* under ASSESS-07-06-02.

TDIF Req: ASSESS-07-06-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* MUST commission an *Assessor* to conduct a *Penetration test* of:

a) its *Identity System*; and

b) each major production release of software forming part of its *Identity System* following accreditation.

7.7 Accessibility assessment

TDIF Req: ASSESS-07-07-01; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Applicant* *MUST* commission an *Assessor* to conduct an *Accessibility Assessment* as part of initial accreditation and annually thereafter as part of the *Annual Assessment,* which *MUST*, at a minimum, assess whether the *Applicant's Identity System*:

- meets *WCAG* version 2.0 to the AA standard for web-based identity services[30]
- meets *WCAG* version 2.1 to the AA standard for mobile-based identity services.

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

Appendix A: Risk ratings

Refer to *ISO 31000 – Risk Management* or the *Applicant's* own risk management framework for a description of likelihood and consequence ratings.

Extreme Risk. The *Applicant* fails to meet a *TDIF* requirement, or an Assessor has identified a risk or recommendation, which results in extreme unmitigated risk.

- An extreme unmitigated risk *MUST* result in a failed *Functional Assessment* as per ASSESS-07-04-03a
- The DTA's delegate will consider immediate suspension of an *Applicant*'s initial accreditation activities, which may occur until such time as the extreme risk is sufficiently mitigated
- The DTA's delegate will consider whether a reaccreditation activity for any evidence already submitted to the DTA is required for the *Applicant*'s *Identity System* once it has confirmed that the extreme risk is sufficiently mitigated as per ASSESS-07-04-03a and ASSESS-07-04-03b.
- If the *Applicant* fails to mitigate the risk or rectify the TDIF non-compliance within the agreed timeframe, then the DTA may terminate the *Applicant*'s request for accreditation[31].

High Risk. The *Applicant* fails to meet a *TDIF* requirement, or an *Assessor* has identified a risk or recommendation, which results in high unmitigated risk.

- A high unmitigated risk *MUST* result in a failed *Functional Assessment* as per ASSESS-07-04-03a
- The DTA's delegate *MUST* consider immediate suspension of an *Applicant*'s initial accreditation activities, which may occur until such time as the high risk is sufficiently mitigated
- The DTA's delegate *MUST* consider whether a reaccreditation activity for any evidence already submitted to the DTA is required for the *Applicant*'s *Identity System* once it has confirmed that the high risk is sufficiently mitigated as per ASSESS-07-04-03a and ASSESS-07-04-03b.
- If the *Applicant* fails to mitigate the risk or rectify the TDIF non-compliance within the agreed timeframe, then the DTA may terminate the *Applicant*'s request for accreditation.

[31] Further information regarding the process of suspended or terminated initial accreditation is available in *TDIF 03 Accreditation Process*

Moderate Risk. The *Applicant* fails to meet a *TDIF* requirement, or an *Assessor* (or equivalent) has identified a risk or recommendation which may result in moderate unmitigated risk.

- A moderate unmitigated risk *MUST* result in a failed *Functional Assessment* as per ASSESS-07-04-03a
- If the *Applicant* fails to mitigate the risk or rectify the TDIF non-compliance within the agreed timeframe, then the DTA may terminate the *Applicant*'s request for accreditation.

Low Risk. The *Applicant* fails to meet a *TDIF* requirement, or an *Assessor* (or equivalent) has identified a risk or recommendation which may result in low unmitigated risk.

- If the *Applicant* fails to mitigate the risk or rectify the TDIF non-compliance within the agreed timeframe, then the DTA may suspend or terminate the *Applicant*'s accreditation[32].

Compliant. The *Applicant* has demonstrated with evidence they comply with a *TDIF* requirement or the intent of a requirement and there are no outstanding risks or recommendations associated with the requirement.

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. The DTA will confirm non-applicability of requirements with the *Applicant*.

[32] Further information is available *in TDIF 07 Maintain Accreditation* regarding assessment of items on an Applicant's *Forward Work Plan*.