Trusted Digital Identity Rules 20XX

I, Stuart Rowland Robert, Minister for Employment, Workforce, Skills, Small and Family Business, make the following rules.

Dated

Stuart Rowland Robert **DRAFT ONLY—NOT FOR SIGNATURE**
Minister for Employment, Workforce, Skills, Small and Family Business

Contents

1 Name

These rules are the *Trusted Digital Identity Rules 20XX*.

2 Commencement

(1) Each provision of these rules specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Colum 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. The whole of these rules	The later of: (a) the day after this instrument is registered; and (b) the day after the day the *Trusted Digital Identity Act 20XX* commences. However, the provisions do not commence at all if the event mentioned in paragraph (b) does not occur.	

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of these rules. Information may be inserted in this column, or information in it may be edited, in any published version of these rules.

3 Authority

These rules are made under *Trusted Digital Identity Act 20XX*.

4 Definitions

(1) A word or phrase defined in the TDIF accreditation rules has the same meaning in these rules.

(2) In these rules:

Act means the *Trusted Digital Identity Act 20XX*.

associated person, of an entity, means any of the following:

(a) a person who:

(i) makes or participates in making decisions that affect the entity's management of digital identity information; or

(ii) has the capacity to affect significantly the entity's management of digital identity information;

or who would be a person mentioned in subparagraph (a) or (b) if the entity were accredited or onboarded to the trusted digital identity system; or

(b) if the person is a body corporate—a person who:
  (i) is an associate (within the meaning of the *Corporations Act 2001*) of the entity; or
  (ii) is an associated entity (within the meaning of the *Corporations Act 2001*) of the entity.

Australian law means a law of the Commonwealth, or of a State or Territory.

banning order has the same meaning as in the *Corporations Act 2001*.

cyber security event means an occurrence of a system, service or network state indicating a possible or actual breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.

cyber security incident means an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.

cyber security risk, in relation to an entity, means the risk that a cyber security incident will occur in relation to the entity.

digital identity fraud incident, in relation to an accredited entity or a participating relying party, means:

(a) in the case of an accredited entity—conduct in connection with a service that the entity is accredited to provide; or
(b) in the case of a participating relying party—conduct in connection with a service provided or received by the participating relying party by or through a digital identity system;

being conduct that:

(c) misrepresents the digital identity of an individual; or
(d) involves fraud in relation to the digital identity of an individual;

because of which the digital identity of an individual, or an attribute or a credential of an individual, is or may be compromised or is or may be unreliable.

digital identity fraud risk, in relation to an accredited entity or a participating relying party, means the risk that a digital identity fraud incident will occur in relation to the accredited entity or participating relying party.

reportable incident means an incident of a kind referred to in any of sections 10 to 16.

reportable incident requirement means a requirement in these rules in respect of a reportable incident.

serious criminal offence means an offence for which, if the act or omission had taken place in the Jervis Bay Territory, a person would have been be liable, on first conviction, to imprisonment for a period of not less than 5 years.

Note: Jervis Bay Territory is mentioned because it is a jurisdiction in which the Commonwealth has control over the criminal law.

5 Fit and proper person considerations

(1) For section 12 of the Act, the following matters are specified in relation to an entity:

(a) whether the entity, or an associated person of the entity, has, within the previous 10 years, been convicted or found guilty of:

(i) a serious criminal offence; or

(ii) an offence of dishonesty;

against an Australian law or a law of a foreign country;

(b) whether the entity, or an associated person of the entity, has been found to have contravened:

(i) an Australian law relevant to the management of digital identity information; or

(ii) a corresponding law of a foreign country;

(c) whether the entity, or an associated person of the entity, has been the subject of:

(i) a determination under paragraph 52(1)(b), or any of paragraphs 52(1A)(a), (b), (c) or (d), of the *Privacy Act 1988*; or

(ii) a corresponding determination under an Australian law or the law of a foreign country;

(d) if the entity is a body corporate—whether a director (within the meaning of the *Corporations Act 2001*) of the entity, or of an associated person of the entity:

(i) has been disqualified from managing corporations; or

(ii) is subject to a banning order;

(e) whether the entity, or an associated person of the entity, has a history of insolvency or bankruptcy;

(f) whether the entity, or an associated person of the entity, has been the subject of a determination made under:

(i) an external dispute resolution scheme recognised under the *Privacy Act 1988*; or

(ii) a similar scheme under a corresponding Australian law or a foreign country;

being a determination that included a requirement to pay monetary compensation;

(g) if the entity has made an application for approval to onboard to the trusted digital identity system or for accreditation as an accredited entity—whether the application was refused;

(h) if the entity is or has been accredited as an accredited entity—whether the accreditation is or has been suspended or revoked;

(j) whether the entity:

(i) has made a false or misleading statement in an application under the Act; or

(ii) has given false or misleading information, documents or evidence to the Oversight Authority;

(k) any other relevant matter, including the objects of the Act.

(2) Subsection (1) does not affect the operation of Part VIIC of the *Crimes Act 1914* or a corresponding provision of an Australian or a law of a foreign country.

Note: Part VIIC of the *Crimes Act 1914* includes provisions that, in certain circumstances, relieve persons from the requirement to disclose spent convictions and require persons aware of such convictions to disregard them.

6 Applications for approval to onboard—all entities

(1) For paragraph 18(1)(g) of the Act, the requirements in this section are prescribed in respect of an entity applying for approval to onboard to the trusted digital identity system.

(2) It is a requirement that the Oversight Authority is satisfied that the entity has effective procedures to notify the Oversight Authority promptly:

(a) in the case of an accredited entity:

(i) of a proposed significant change (including new software releases) to its accredited facility; and

(ii) of the effect that the proposed change will or is expected to have on the operation of the entity's accredited facility and of the trusted digital identity system; and

(b) in the case of a relying party:

(i) of a proposed significant change (including new software releases) to its facility; and

(ii) of the effect that the proposed change will or is expected to have on the operation of its facility and of the trusted digital identity system; and

(c) in either case—of outages or downtime affecting a facility mentioned in paragraph (a) or (b) or affecting access by any person to the trusted digital identity system.

(3) It is a requirement that the Oversight Authority is satisfied that the entity has effective procedures to measure accurately the extent to which the entity achieves applicable service levels determined by the Oversight Authority under paragraph 87(c) or (d) of the Act.

(4) It is a requirement that the Oversight Authority is satisfied that the entity has effective procedures to notify the Oversight Authority promptly of incidents adversely affecting the entity which may lead to a degradation of or loss of functionality in the trusted digital identity system.

7 Applications for approval to onboard—relying parties

(1) For paragraph 18(1)(g) of the Act, the following requirements are prescribed in respect of an entity applying for approval to onboard to the trusted digital identity system as a participating relying party:

(a) the entity must have a written plan for testing (within periods and at intervals specified in the plan) the interoperability of its facility and the trusted digital identity system;

(b) the entity must have conducted a cyber security risk assessment in relation to its integration of its facility with the trusted digital identity system;

(c) the entity must have adopted written processes and procedures:

(i) to investigate digital identity fraud incidents in relation to its facility, including incidents notified to it by the Oversight Authority; and

(ii) to ensure its compliance with section 44 of the Act;

(iii) to prevent, identify and investigate unauthorised access, including by the entity's personnel and contractors, to digital identity information under the entity's control;

(d) the entity must have effective procedures to ensure that it complies with the reportable incident requirements;

(e) the entity must have adopted a business continuity plan that addresses at least the following:

(i) disaster recovery procedures;

(ii) continuity procedures for critical functions of its digital identity facility;

(iii) regular reviews of the plan, but at least once a year;

(iv) procedures for notifying the Oversight Authority of changes to the plan and results of periodic reviews;

(f) the entity must have effective programs to prevent, detect, investigate and report cyber security incidents, and digital identity fraud incidents, in relation to its facility.

Note For subparagraph (1)(c)(ii): section 44 of the Act relates to the redress obligations of participating relying parties.

(2) The programs mentioned in paragraph (1)(f) must include the following measures:

(a) the conduct of regular assessments of the risk concerned;

(b) the adoption of a comprehensive and effective cyber security and digital identity fraud control plan;

(c) the maintenance of registers of cyber security risks and digital identity fraud risks;

(d) appropriate staff training in matters of cyber security and digital identity fraud control.

8 Conditions on approval to onboard

For subsection 22(7) of the Act, for an approval of an entity described in an item of the following table, it is determined that the conditions in that item are included in the approval.

Item	Entity	Condition
1	An accredited identity exchange	The identity exchange must have, as part of its accredited facility, a user dashboard that meets the requirements of the TDIF accreditation rules.

Item	Entity	Condition
2	A participating relying party	The relying party must notify the Oversight Authority of any proposed change in its contact details, and must do so no later than 28 days before the change takes effect.
3	A participating relying party	The relying party must not disclose to another relying party (whether or not a participating relying party): (a) an attribute of an individual; or (b) a restricted attribute; unless permitted by another condition included in the approval,

9 Holding etc. digital identity information outside Australia

(1) This section applies to each of the following:

(a) an entity that holds an approval to onboard to the trusted digital identity system;

(b) an entity whose approval to onboard to the trusted digital identity system is suspended or has been revoked.

Note This section applies to digital identity information generated, collected, held or stored by accredited entities within the trusted digital identity system (section 31 of the Act).

(2) For section 31 of the Act, an entity must not engage in, or cause or permit another person to engage in, the following conduct:

(a) holding, storing or handling digital identity information at a place outside Australia; or

(b) transferring digital identity information to a place outside Australia for storage, processing or handling;

unless an exemption under subsection (4) is in force for the entity in relation to the conduct.

(3) Subsection (2) does not apply in relation to:

(a) conduct undertaken to comply with a request by the individual to whom the digital identity information relates, being a request made from a place outside Australia; or

(b) conduct undertaken to verify the identity of an individual or authenticate the digital identity of, or information about, an individual.

(4) The Oversight Authority may, on application by an entity mentioned in subsection (1), grant the entity an exemption in respect of conduct, or specified conduct, prohibited by subsection (2). The exemption may be subject to conditions specified in the exemption.

(5) In considering whether to grant an exemption to an entity:

(a) the matters that the Oversight Authority must consider include:.

(i) any risk assessment plan provided by the entity; and

(ii) any privacy impact assessment provided by the entity, so far as it relates to personal information that may be disclosed under the proposed exemption; and

(ii) the effectiveness of the entity's protective security (including security governance, information security, personnel security and physical security) and fraud control arrangements; and

(b) the matters that the Oversight Authority may consider include whether the technology required by the entity is available in Australia or is available to the entity in Australia.

(6) For subsection 133(2) of the Act:

(a) a decision under subsection (4) to refuse to grant an exemption to an entity is a reviewable decision and the entity that applied for the exemption is affected by the decision; and

(b) a decision under subsection (4) to impose conditions on an exemption granted to an entity is a reviewable decision and the entity that applied for the exemption is affected by the decision.

10 Reportable incidents—cyber security incidents

(1) The arrangements described in this section are prescribed for subsection 32(1) of the Act.

(2) The arrangements described in this section apply to:

(a) an onboarded entity; and

(b) an entity whose approval to onboard is suspended; and

(c) an entity whose approval to onboard has been revoked, but only in respect of incidents that occurred while the entity was onboarded to the trusted digital identity system.

(3) The entity must notify the Oversight Authority, in accordance with this section, of the following kinds of incidents in relation to the trusted digital identity system:

(a) cyber security incidents in relation to:

(i) for an accredited entity—the services provided by the entity as an accredited entity or the entity's accredited facility; or

(ii) in the case of a participating relying party—its operations in the trusted digital identity system or its facility;

(b) incidents that the entity suspects or ought reasonably to suspect are incidents described in paragraph (a).

(4) A notification by an entity must include the following information:

(a) the entity's name;

(b) the contact details of the entity;

(c) if the entity is accredited as more than one kind of accredited entity—the service affected by the incident;

(d) a description of the incident;

(e) the following details of the incident, so far as they are known to the entity:

(i) the date and time of the incident;

(ii) the date on which the entity became aware of the incident;
(iii) the method or source of detection of the incident;
(iv) the severity of the incident;
(v) whether the incident has been resolved;
(vi) if the incident has been resolved—how it was resolved and how long the entity took to resolve it;

(f) if the entity is aware of other similar incidents within the previous 12 months—the number of those incidents;

(g) if the entity is an identity service provider:
(i) the digital identities affected by the incident; and
(ii) the attributes and credentials of those identities; and
(iii) the contact details for each of the users whose digital identities are affected by the incident, so far as they are known to the entity;

(h) for each individual whose digital identity is affected by the incident:
(i) whether the individual has been informed of the incident; and
(ii) what steps the entity has taken or proposes to take to comply with Division 3 of Part 3 of Chapter 2 of the Act in relation to the incident;

(i) any relevant identity proofing level and credential level;

(j) the measures that the entity has taken and plans to take to deal with the incident, including action taken or to be taken to reduce risk to the entity's accredited facility or to the facility in respect of which the entity is onboarded;

(k) whether the incident has been referred to an enforcement body and, if so, to which;

(l) if the entity is a participating relying party—the pairwise identifier associated with the incident.

(5) A notification of an incident must be made as soon as practicable after, and in any event no later than 24 hours after, the entity becomes aware of the incident. The notification may be oral.

(6) If the entity is not able to provide some or all of the information required by subsection (4) in relation to an incident, so that it is not practicable for the entity to comply fully with that subsection within the period specified in subsection (5), the entity is taken to comply with subsection (4) if:

(a) it takes reasonable steps to obtain the missing information as soon as possible; and

(b) it provides an interim notification by the time required by subsection (5) with as much of the required information as is available to it; and

(c) at intervals of no longer than 48 hours thereafter—it notifies additional required information as is available to it; and

(d) the entity completes the notification as soon as practicable after making the interim notifications.

11 Reportable incidents—digital identity fraud incidents

(1) The arrangements described in this section are prescribed for subsection 32(1) of the Act.

(2) The arrangements described in this section apply to:
  (a) an onboarded entity; and
  (b) an entity whose approval to onboard is suspended; and
  (c) an entity whose approval to onboard has been revoked, but only in respect of incidents that occurred while the entity was onboarded.

(3) The entity must notify the Oversight Authority, in accordance with this section, of the following kinds of incidents in relation to the trusted digital identity system:
  (a) digital identity fraud incidents in relation to:
    (i) for an accredited entity—the services provided by the entity as an accredited entity or the entity's accredited facility; or
    (ii) for a participating relying party—its operations in the trusted digital identity system or its facility;
  (b) incidents that the entity suspects or ought reasonably to suspect are incidents as described in paragraph (a).

(4) A notification of an incident by an entity must include the following information:
  (a) the entity's name;
  (b) the contact details of the entity;
  (c) if the entity is accredited as more than one kind of accredited entity—the service affected by the incident;
  (d) a description of the incident;
  (e) the following details of the incident, so far as they are known to the entity:
    (i) the date and time of the incident;
    (ii) the date on which the entity became aware of the incident;
    (iii) the method or source of detection of the incident;
    (iv) the severity of the incident;
    (v) whether the incident has been resolved;
    (vi) if the incident has been resolved—how it was resolved and how long the entity took to resolve it;
  (f) if the entity is aware of other similar incidents within the previous 12 months—the number of those incidents;
  (g) if the entity is an identity service provider—the digital identities affected by the incident;
  (h) for each individual whose digital identity is affected by the incident:
    (i) whether the individual has been informed of the incident; and
    (ii) what steps the entity has taken or proposes to take to comply with Division 3 of Part 3 of Chapter 2 of the Act in relation to the incident;
  (i) any relevant identity proofing level and credential level;
  (j) the measures that the entity has taken and plans to take to deal with the incident, including action taken or to be taken to reduce risk to the entity's digital identity system or the relevant accredited facility or facility;
  (k) whether the incident has been referred to an enforcement body and, if so, to which;
  (l) if the entity is a participating relying party—the pairwise identifier associated with the incident.

(5) A notification of an incident must be made as soon as practicable after, and in any event no later than 24 hours after, the entity becomes aware of the incident. The notification may be oral.

(6) If the entity is not able to provide some or all of the information required by subsection (4) in relation to an incident, so that it is not practicable for the entity to comply fully with that subsection within the period specified in subsection (5), the entity is taken to comply with subsection (4) if:
  (a) it takes reasonable steps to obtain the missing information as soon as possible; and
  (b) it provides an interim notification by the time required by subsection (5) with as much of the required information as is available to it; and
  (c) at intervals of no longer than 48 hours thereafter—it notifies additional required information as is available to it; and
  (d) the entity completes the notification as soon as practicable after making the interim notifications.

12 Reportable incidents—changes in control of onboarded corporations

(1) The arrangements described in this section are prescribed for subsection 32(1) of the Act.

(2) This section applies to:
  (a) an entity that is an onboarded corporation; and
  (b) an entity that is a corporation whose approval to onboard is suspended;
but does not apply to a corporation that is controlled by the Commonwealth, a State or Territory or an authority of a State or Territory.

(3) The entity must notify the Oversight Authority, in accordance with this section, of a change in control of the entity (within the meaning of section 910B of the *Corporations Act 2001*).

(4) A notification of a change in control of an entity must include the following information:
  (a) the entity's name;
  (b) the contact details for the entity;
  (c) if the entity is accredited as more than one kind of accredited entity—the service affected by the incident;
  (d) the following details in respect of each entity that, through the change or proposed change in control of the entity, has started or would start to control the entity (***incoming entity***):
    (i) the name of the incoming entity;
    (ii) the incoming entity's ABN or ARBN;
    (iii) the address of the incoming entity's principal place of business;
    (iv) the other contact details of the incoming entity;
    (v) if the incoming entity was incorporated outside Australia—the location of its incorporation and the address of its principal place of business in Australia;
    (vi) the business names of the incoming entity;

(vii) the date on which the incoming entity was registered under the *Corporations Act 2001* or the law of a State or Territory under which the incoming entity was incorporated or registered;

(viii) the names and addresses of each of the directors and other officers of the incoming entity;

(ix) in respect of each subsidiary (as defined in section 9 of *Corporations Act 2001*) of the incoming entity—the information specified in subparagraphs (i) to (viii);

(e) the date on which the change of control occurred or is proposed to occur;

(f) if the incoming entity is accredited or holds an approval to onboard—details of that accreditation or approval.

(4) A notification required by subsection (1) must be made:

(a) if the entity becomes aware of a proposal for the change in control before it occurs—within 24 hours after the entity becomes aware; or

(b) otherwise—within 24 hours after the change in control occurs.

(5) In this section:

corporation has the meaning given in the *Corporations Act 2001*.

director has the meaning given in section 9 of the *Corporations Act 2001* and, for that purpose, ***body*** has the meaning given in that section.

officer has the meaning given in section 9 of the *Corporations Act 2001*.

subsidiary has the meaning given in section 9 of the *Corporations Act 2001*.

13 Reportable incidents—changes in contractors

(1) The arrangements described in this section are prescribed for subsection 32(1) of the Act.

(2) The arrangements described in this section apply to an onboarded entity.

(3) The entity must notify the Oversight Authority, in accordance with this section, of the proposed engagement by the entity of a contractor to provide, on behalf of the entity, a service for which the entity is accredited, or part of such a service, being a service within the trusted digital identity system .

(4) A notification by an entity must include the following information:

(a) the entity's name;

(b) the contact details for the entity;

(c) if the entity is accredited as more than one kind of accredited entity—the service affected by the incident;

(d) the following details in respect of the contractor (***incoming contractor***):

(i) the name of the incoming contractor;

(ii) the incoming contractor ABN or ARBN;

(iii) the address of the incoming contractor's principal place of business;

(iv) if the incoming contractor was incorporated outside Australia—the location of its incorporation and the address of its principal place of business in Australia;

(v) the business names of the incoming contractor;

(e) the date on which the engagement is proposed to start;

(f) the date on which the engagement is proposed to end;

(g) the names of each of the incoming contractor's key persons relevant to the engagement or proposed engagement;

(h) a statement whether the contract under which the incoming contractor is or is proposed to be engaged requires the contractor to ensure that its activities under the contract do not result in the entity contravening the Act, these rules or the TDIF accreditation rules.

(3) A notification required by subsection (1) must be made no later than 28 days before the engagement is proposed to start.

(4) Subsection (1) does not apply if the proposal to engage the incoming contractor has previously been notified to the Oversight Authority, including in the entity's application for onboarding.

14 Reportable incidents—events and circumstances related to "fit and proper" considerations

(1) The arrangements described in this section are prescribed for subsection 32(1) of the Act.

(2) The arrangements described in this section apply to:

(a) an onboarded entity; and

(b) an entity whose approval to onboard is suspended.

(1) An entity must notify the Oversight Authority, in accordance with this section, of an event or circumstance of a kind described in section 5 that occurs or arises in relation to the entity or to an associated person of the entity.

(3) A notification by an entity must include the following information:

(a) the entity's name;

(b) the contact details for the entity;

(c) if the event or circumstance relates to an associated person of the entity—the name and contact details of the associated person;

(d) the details of the event or circumstance, including:

(i) when it occurred or arose; and

(ii) its nature; and

(iii) sufficient other details to enable the Oversight Authority to determine whether the Authority should take any action in relation to the entity's approval to onboard.

(4) A notification of an incident under this section must be made no later than 7 days after the entity becomes aware of the incident.

15 Reportable incidents—changes in use of trusted digital identity system

(1) The arrangements described in this section are prescribed for subsection 32(1) of the Act.

(2) The arrangements described in this section apply to:
  (a) an onboarded accredited entity; and
  (b) an accredited entity whose approval to onboard is suspended.

(3) If an entity proposes to do either of the following:
  (a) use its accredited facility in or with a digital identity system other than the trusted digital identity system;
  (b) use a digital identity generated by the trusted digital identity system in another digital identity system;

the entity must notify the Oversight Authority, in accordance with this section, of the proposal.

(5) A notification by an entity must include the following information:
  (a) the entity's name;
  (b) the contact details for the entity;
  (c) if the entity is accredited as more than one kind of accredited entity and the service to be provided in the other digital identity system is of the same kind as a service it is accredited to provide in the trusted digital identity system—a description of the service to be provided in the other digital identity system;
  (d) details of the entity providing or managing the other digital identity system;
  (e) the nature of the proposed use of the other digital identity system;
  (f) the likely effect of using the other digital identity system on the levels of the entity's cyber security risk and digital identity fraud risk;
  (g) details of how the entity will distinguish between services provided in the trusted digital identity system and those provided in the other digital identity system;
  (h) details of how the entity will ensure that digital identity information held in the trusted digital identity system will not be able to be accessed for, or used in, the other digital identity system.

Example For paragraph (h): an information barrier.

(6) A notification required by subsection (1) must be made no later than 28 days before the entity proposes to use the other digital identity system as described in subsection (3).

16 Reportable incidents—increase in use of trusted digital identity system

(1) The arrangements described in this section are prescribed for subsection 32(1) of the Act.

(2) The arrangements described in this section apply to an entity that is a participating relying party.

(3) If:

(a) the number of transactions during a month, being transactions that involve the trusted digital identity system and users of the participating relying party's facility, is 10% or more than the average number of such transactions occurring in each of the previous 6 months; and

(b) it is reasonable to expect that that level of use will continue or increase in the next 3 months;

the participating relying party must notify the Oversight Authority, in accordance with this section, of the increase.

(4) A notification by a participating relying party must include the following information:

(a) its name;

(b) its contact details;

(c) the extent of the increase;

(d) the reasons for the increase, so far as they are known to the participating relying party.

(4) The notification under this section must be made no later than 7 days after the end of the month concerned.

17 Reportable incidents—Oversight Authority may disclose information

The Oversight Authority may give information notified to it about a cyber security incident, digital identity fraud incident or increase in use of the trusted digital identity system to any or all of the following:

(a) an onboarded entity;

(b) the Minister;

(c) an enforcement body;

if the Oversight Authority considers it necessary to do so to protect the security, integrity or performance of the trusted digital identity system.

18 Reportable incidents—requirements for action for entities

(1) This section applies if a reportable incident occurs in relation to an entity and so applies whether or not the incident has been notified as required by these rules.

(2) If the incident is a cyber security incident, the entity must take reasonable steps to:

(a) mitigate the adverse effects of the incident; and

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

(3) The entity must comply with any direction, request or requirement given in writing by the Oversight Authority to provide specified information about the incident to the Oversight Authority.

19 Record keeping by onboarded entities and former onboarded entities

(1) For subsection 131(3) of the Act, records that include prescribed information are prescribed.

(2) For subsection 131(3) of the Act:

(a) in respect of a record of an entity whose onboarding approval has been revoked—the period of 3 years after the record was created is prescribed; and

(b) in respect of other records—the period of 7 years after the record was created is prescribed.

(3) If 2 periods apply under this section in respect of a record, each period applies separately.

(4) Subsections (1) and (2) do not relate to records of a kind that do not relate to information obtained by entities through the trusted digital identity system.

(5) In this section:

prescribed information means digital identity information that meets the requirements of rules 4.2.6(5) to 4.2.6(9) of the TDIF accreditation rules.