Digital ID Rules 2024

I, Katy Gallagher, Minister for Finance, make the following rules.

Dated

Katy Gallagher **DRAFT ONLY—NOT FOR SIGNATURE**
Minister for Finance

Contents

Chapter 1—Preliminary

1.1 Name

These rules are the *Digital ID Rules 2024*.

1.2 Commencement

These rules commence at the same time as the *Digital ID Act 2024* commences.

1.3 Authority

These rules are made under section 168 of the *Digital ID Act 2024* for the purposes of that section and the provisions in the Act in which the term 'Digital ID Rules' occurs.

1.4 Definitions

Note: Some expressions used in these rules are defined in the Act, including:

- Accreditation Rules;
- accredited entity;
- accredited identity exchange provider;
- accredited identity service provider;
- accredited service;
- Australia;
- Australian Government Digital ID System;
- cyber security incident;
- digital ID;
- Digital ID Accredited Entities Register;
- Digital ID Data Standards;
- digital ID fraud incident;
- Digital ID Regulator;
- digital ID system;
- digital ID trustmark;
- enforcement body;
- entity;
- law enforcement agency;
- participating relying party;
- personal information; restricted attribute.

In these rules:

Accreditation Data Standards means the *Digital ID (Accreditation) Data Standards 2024*.

Act means the *Digital ID Act 2024*.

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

(a) a person who makes, or participates in making, decisions that affect:

(i) the entity's management of its DI data environment; or

(ii) for a participating relying party—the performance of the entity's functions when operating in the Australian Government Digital ID System; or

(b) a person who has the capacity to significantly affect:

(i) the entity's management of its DI data environment; or

(ii) for a participating relying party—the performance of the entity's functions when operating in the Australian Government Digital ID System; or

(c) a person who would be a person mentioned in paragraphs (a) or (b) if the entity was an accredited entity or a participating relying party; or

(d) if the entity is a body corporate—a person who:

(i) is an associate (within the meaning of the Corporations Act) of the entity; or

(ii) is an associated entity (within the meaning of the Corporations Act) of the entity.

authentication level has the same meaning as in the Accreditation Data Standards.

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

Corporations Act means the *Corporations Act 2001*.

DI data environment means the information technology systems used for, and the processes that relate to, the provision of an entity's accredited services or, for an applicant for accreditation, the accredited services the entity proposes to provide.

identity proofing level means a level specified in the first row of the table in rule 5.12 of the Accreditation Rules.

material change has its ordinary meaning.

material effect, in relation to the operation of the Australian Government Digital ID System, includes:

(a) any degradation or loss of functionality within the Australian Government Digital ID System; and

(b) any detrimental effect on the ability of an entity that participates in the Australian Government Digital ID System to access the System.

participating entity means an entity that holds an approval to participate in the Australian Government Digital ID System.

Privacy Act means the *Privacy Act 1988*.

pairwise identifier means an identifier that identifies the individual to either an identity exchange provider or a participating relying party that cannot be correlated with another individual's pairwise identifier or that individual's pairwise identifier used at a different system participant.

public-facing accredited services means the accredited services or elements of an entity's information technology system that an individual directly interacts with when using, or attempting to use, the entity's accredited services.

Example: An example of public-facing accredited services is where an individual provides information to be verified via an accredited identity service provider's mobile app that the individual is required to download so as to access the entity's accredited services.

public-facing information related to accredited services means information made available by the accredited entity to individuals when interacting with the entity's public-facing accredited services.

Example: Public-facing information related to accredited services is the accredited entity's privacy policy made available to individuals.

reportable incident requirement means a requirement in these rules in respect of an incident specified in Chapter 4.

service levels mean the service levels determined under section 80 of the Act.

statutory contract means the contract taken to be in force under subsection 85(1) of the Act.

Chapter 2—Fit and proper person considerations

2.1 Application of this Chapter

(1) For the purposes of subsection 12(a) of the Act, this Chapter specifies the matters to which the Digital ID Regulator must have regard when considering whether the person is a fit and proper person for the purposes of the Act, these rules, the Accreditation Rules, the Digital ID Data Standards and the service levels.

Note: In deciding whether to accredit an entity, suspend or revoke the accreditation of an entity, approve an entity to participate in the Australian Government Digital ID System, or suspend or revoke the approval of an entity to participate in the Australian Government Digital ID System, the Digital ID Regulator may have regard to whether the entity is a fit and proper person (see subsections 15(5), 25(4), 26(3), 62(2), 71(3) and 72(3) of the Act).

(2) For the avoidance of doubt, this Chapter does not limit the matters to which the Digital ID Regulator may have regard when considering whether the person is a fit and proper person for the purposes of the Act, these rules, the Accreditation Rules, the Digital ID Data Standards and the service levels.

2.2 Mandatory relevant matters

(1) In having regard to whether an entity is a fit and proper person, the Digital ID Regulator must have regard to the following matters:

(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 any law of the Commonwealth or of a State or Territory, or a law of a foreign jurisdiction;

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

(i) a law relevant to the management of its DI data environment; or

(ii) a similar law of a foreign jurisdiction;

(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 paragraph 52(1A)(a), (b), (ba), (c) or (d), of the Privacy Act; or

(ii) a finding or determination of a similar nature under a similar law of a State or Territory or a foreign jurisdiction;

(d) if the entity is a body corporate—whether any of the directors (within the meaning of the Corporations Act) 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 an external dispute resolution scheme that:
  (i) included a requirement to pay compensation; and
  (ii) was, at the time the determination was made:
    (A) recognised under section 35A of the Privacy Act; or
    (B) recognised under section 56DA of the *Competition and Consumer Act 2010*;

(g) if the entity has made an application under section 14 of the Act for accreditation as an accredited entity—whether the application was refused;

(h) if the entity has made an application under section 61 of the Act for approval to participate in the Australian Government Digital ID System—whether the application was refused;

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

(j) if the entity is or has been approved to participate in the Australian Government Digital ID System—whether the approval is or has been suspended or revoked.

(2) Subrule (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.

(3) In this rule:

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

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 liable, on first conviction, to imprisonment for a period of not less than 5 years.

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

Chapter 3—Participation in the Australian Government Digital ID System

Part 1—Applications for approval to participate

3.1 Application of this Part

(1) For the purposes of paragraph 62(1)(f) of the Act, an entity that has made an application under section 61 of the Act for approval to participate in the Australian Government Digital ID System must meet the requirements in this Part.

Note: An application made under section 61 of the Act must be accompanied by any information or documents required by this Part (see paragraph 141(1)(c) of the Act). The Digital ID Regulator is not required to make a decision on the application until the information or documents are provided (see subsection 143(2) of the Act).

3.2 Applications for approval to participate—all entities

(1) An entity that has made an application for approval to participate in the Australian Government Digital ID System must establish, to the satisfaction of the Digital ID Regulator, that it has effective written procedures to notify the System Administrator promptly of:

(a) any proposed change to the entity's information technology system that interacts with the Australian Government Digital ID System, where the change will, or could reasonably be expected to, have a material effect on the operation of the Australian Government Digital ID System; and

(b) any planned or unplanned outage or downtime affecting the entity's information technology system, where the outage or downtime will, or could reasonably be expected to, have a material effect on the operation of the Australian Government Digital ID System.

(2) The application must be accompanied by any information or documents necessary to satisfy the Digital ID Regulator of the matters in subrule (1).

3.3 Applications for approval to participate—relying parties

[Consultation note: The requirements included in this rule 3.3 are based on existing requirements applicable to Government entities seeking to onboard to the Australian Government Digital ID System. They are designed to ensure that the System Administrator and the government relying parties reach an agreement prior to onboarding on how different types of incidents relating to the AGDIS are managed, so that if an incident occurs these can be resolved effectively.

We are seeking feedback on how to achieve this coordinated response in future phases of the AGDIS rollout, where non-Government organisations who may not have large fraud and security teams may find these requirements difficult to meet.]

(1) Before a relying party applies for approval to participate in the Australian Government Digital ID System, the entity must conduct a risk assessment to identify, evaluate and manage the risks of:

(a) a cyber security incident; and

(b) a digital ID fraud incident;

occurring in connection with a service that the entity intends to provide, or provide access to, within the Australian Government Digital ID System.

(2) A relying party that has made an application for approval to participate in the Australian Government Digital ID System must, at the time it makes the application, have all of the following:

(a) a written cyber security plan approved by the entity's governing body that addresses at least the following:

(i) management of any risks identified when conducting the risk assessment at paragraph (1)(a);

(ii) prevention, identification, investigation and management of cyber security incidents, including incidents notified to the entity by the System Administrator, if the entity is approved to participate in the Australian Government Digital ID System; and

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

(b) a written digital ID fraud management plan approved by the entity's governing body that addresses at least the following:

(i) management of any risks identified when conducting the risk assessment at paragraph (1)(b);

(ii) prevention, identification, investigation and management of digital ID fraud incidents, including incidents notified to the entity by the System Administrator, if the entity is approved to participate in the Australian Government Digital ID System; and

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

(c) a written disaster recovery and business continuity plan approved by the entity's governing body that addresses at least the following:

(i) disaster recovery procedures for critical functions of the entity's information technology system within the Australian Government Digital ID System; and

(ii) regular reviews of the plan, but at least once per year.

(3) The application must be accompanied by any information or documents necessary to satisfy the Digital ID Regulator of the matters in subrules (1) and (2).

Part 2—Approval to participate

3.4 Conditions on approval to participate

(1) For the purposes of subsection 64(5) of the Act, the approval of an entity described in column 1 of an item of the following table is subject to the conditions specified in column 2 of the item in the circumstances (if any) specified in column 3 of the item.

Participation conditions			
Item	**Column 1** **Entity**	**Column 2** **Condition**	**Column 3** **Circumstances**
1	Participating relying party	The entity must notify the Digital ID Regulator of a proposed change to its contact details no later than 7 days after the change takes effect.	
2	Participating relying party	The entity must notify the System Administrator, in accordance with subrule (2), of the following incidents: (a) any proposed change to the entity's information technology system that interacts with the Australian Government Digital ID System, where the change will, or could reasonably be expected to, have a material effect on the operation of the Australian Government Digital ID System; and (b) any planned or unplanned outage or downtime affecting the entity's information technology system, where the outage or downtime will, or could reasonably be expected to, have a material effect on the operation of the Australian Government Digital ID System. The notification must be made no later than 5 business days after the entity becomes aware of the incident or a suspected incident.	
3	Participating relying party	The entity must collect and store the pairwise identifier issued to the relying party in relation to each individual to enable the entity to comply with the reportable incident requirement mentioned in paragraph 4.2(3)(k).	
4	Participating relying party	The entity must notify the Digital ID Regulator if the entity becomes or ceases to be a 'reporting entity' (within in the meaning of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*) as soon as practicable, and in any event no later than 7 days after the change takes effect.	
5	Participating relying party	The entity may collect and disclose the following restricted attributes of an individual: (a) Australian or foreign passport number; (b) Australian or foreign driver's licence	Where the collection and disclosure by the entity: (a) is for the purpose of the entity complying with its obligations under the *Anti-Money Laundering*

Participation conditions			
Item	**Column 1** **Entity**	**Column 2** **Condition**	**Column 3** **Circumstances**
		number; (c) Australian visa grant number; (d) Australian proof of age card number; (e) Medicare card number (within the meaning of Part VII of the *National Health Act 1953*); if the entity is a 'reporting entity' (within in the meaning of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*) at the time of the collection.	*and Counter-Terrorism Financing Act 2006*; and (b) complies with the requirements of the Act (including Division 2 of Part 2 of Chapter 3).
6	Accredited identity service provider	The entity may: (a) collect the following restricted attributes of an individual: (i) Australian or foreign passport number; (ii) Australian or foreign driver's licence number; (iii)Australian visa grant number; (iv)Australian proof of age card number; (v) Medicare card number (within the meaning of Part VII of the *National Health Act 1953*); and (b) disclose the restricted attributes of an individual mentioned in paragraph (a) to a participating relying party.	Where the collection and disclosure by the entity: (a) is for the purpose of the participating relying party complying with its obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*; and (b) complies with the requirements of the Act (including Division 2 of Part 2 of Chapter 3).
7	Accredited entity	The entity must warrant to all other parties to the statutory contract that the use by a person specified in subrule (3) of an item provided or made available by the first party for use within the Australian Government Digital ID System does not infringe the intellectual property rights of the first party or any person that is not a party to the contract.	

(2) The notification must include the following information:

(a) the entity's name;

(b) the contact details for the entity;

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

(d) a description of the incident;

(e) the following details of the incident:

(i) the date and time of the incident;

(ii) the date on which the entity became aware of the incident; and

(iii) sufficient other details to enable the Digital ID Regulator to determine whether the Regulator should take any action in relation to the entity's approval to participate.

(3) For the purposes of item 7 of the table in subrule (1), the specified persons are:

(a) any other party to the statutory contract;

(b) a contractor to an entity mentioned in paragraph (a).

(4) In this rule:

intellectual property rights includes 'moral rights' as defined in the *Copyright Act 1968*.

Part 3—Statutory contract

3.5 Intellectual property rights

(1) For the purposes of paragraph 85(1)(d) of the Act, it is a requirement that an accredited entity that is a party to the statutory contract gives the warranty mentioned in item 7 of the table in subrule 3.4(1).

Note: An accredited entity participating in the Australian Government Digital ID System is protected from liability in certain circumstances (see section 84 of the Act and Chapter 7 of these rules).

Chapter 4—Reportable incidents

4.1 Application of this Chapter

(1) For the purposes of subsection 78(1) of the Act, this Chapter prescribes arrangements relating to the notification and management of incidents that have occurred, or are reasonably suspected of having occurred, in relation to the Australian Government Digital ID System.

Note: An entity is liable to a civil penalty if the entity is subject to a requirement under rules made for the purposes of subsection 78(1) and the entity fails to comply with the requirement (see subsection 78(4) of the Act).

4.2 Cyber security incidents and digital ID fraud incidents

(1) This rule applies to:
  (a) a participating entity;
  (b) an entity whose approval to participate is suspended; and
  (c) an entity whose approval to participate has been revoked, but only in respect of incidents that have occurred, or are reasonably suspected of having occurred, while the entity was participating in the Australian Government Digital ID System.

(2) The entity must notify the System Administrator, in accordance with this rule, of any of the following:
  (a) a cyber security incident; or
  (b) a digital ID fraud incident;

where the incident occurred, or is reasonably suspected of having occurred, in relation to any accredited services:
  (c) for an accredited entity—provided by the entity within the Australian Government Digital ID System; or
  (d) for a participating relying party—received by the entity within the Australian Government Digital ID System.

(3) The notification must include the following information:
  (a) the entity's name;
  (b) the contact details of the entity;
  (c) the services 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; and
    (vi) if the incident has been resolved—how it was resolved and how long the entity took to resolve it;

(f) each digital ID affected by the incident;
(g) for each individual whose digital ID is affected by the incident—whether the individual has been informed of the incident and, if so, when;
(h) any relevant identity proofing level and authentication level and, if an individual's digital ID has been re-proofed because of the incident, the date that occurred;
(i) 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 accredited services the entity provides or receives within the Australian Government Digital ID System;
(j) whether the incident has been referred to an enforcement body or law enforcement agency and, if so, to which body or agency and when; and
(k) if the entity is a participating relying party—the pairwise identifier issued to the relying party in relation to each individual associated with the incident.

(4) The notification must be made as soon as practicable after, and in any event no later than 1 business day after, the entity becomes aware of the incident or a suspected incident.

(5) The notification may be given orally. However, if it is given orally, a written notification must be given within 3 working days after the oral notification.

(6) If the entity is not able to provide some or all of the information (***required information***) required by subrule (3), because it is not reasonably practicable for the entity to comply fully with that subrule within the period specified in subrule (4) or (5), the entity is taken to comply with subrule (3) if the entity:
(a) provides an interim notification by the time required by subrule (4) or (5) with as much of the required information as is available to it;
(b) takes reasonable steps to obtain the outstanding required information as soon as reasonably practicable;
(c) at intervals of no longer than 48 hours after the interim notification is provided in accordance with paragraph (a)—provides the outstanding required information as is available to it; and
(d) provides all outstanding required information as soon as reasonably practicable after making the interim notification.

4.3 Changes in control of corporations

(1) Subject to subrule (2), this rule applies to:
(a) a participating entity that is a corporation; and
(b) an entity that is a corporation whose approval to participate is suspended;

(2) This rule does not apply to a corporation that is controlled by:
(a) the Commonwealth or an authority of the Commonwealth;
(b) a State or an authority of that State; or
(c) a Territory or an authority of that Territory.

(3) However, this rule applies to a corporation mentioned in subrule (2) if, as a result of a change in control, or a future change in control, the corporation ceases to be, or will cease to be, controlled by:

(a) for a corporation controlled by an entity mentioned in paragraph (2)(a)—an entity mentioned in paragraph (2)(a);

(b) for a corporation controlled by an entity mentioned in paragraph (2)(b)—an entity mentioned in paragraph (2)(b); or

(c) for a corporation controlled by an entity mentioned in paragraph (2)(c)—an entity mentioned in paragraph (2)(c).

(4) The entity must notify the Digital ID Regulator, in accordance with this rule, of a change in control, or a future change in control, of the entity.

(5) The notification must include the following information:

(a) the entity's name;

(b) the contact details for the entity;

(c) the following details in respect of each entity that, through the change or future 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 name or names of the incoming entity;

(vii) the date on which the incoming entity was registered under the Corporations Act or other law;

(viii) the names and director identification number of each of the directors and other officers of the incoming entity;

(ix) in respect of each subsidiary of the incoming entity—the information specified in subparagraphs (i) to (viii); and

(d) the date on which the change of control occurred or is expected to occur.

(6) The notification must be made:

(a) if the entity becomes aware that, at any time in the future, a change in control of the entity will occur—within 72 hours after the entity becomes aware; or

(b) otherwise—within 72 hours after the change in control occurs.

(7) Without limiting paragraph (6)(a), an entity is taken to be aware that a change in control of the entity will occur at the time:

(a) a resolution is passed by the entity regarding the change in control; or

(b) a court order regarding the change in control is made.

(8) In this rule:

ABN has the meaning given in section 9 of the Corporations Act.

ARBN has the meaning given in section 9 of the Corporations Act.

Commonwealth company has the meaning given in the *Public Governance, Performance and Accountability Act 2013*.

control:

(a) in relation to a ***Commonwealth company***—has the meaning given in section 89 of the *Public Governance, Performance and Accountability Act 2013*;

(b) otherwise—has the meaning given in section 910B of the Corporations Act.

corporation has the meaning given in the Corporations Act.

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

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

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

4.4 Change in contractor

(1) This rule applies to an accredited entity that holds an approval to participate.

(2) The entity must notify the Digital ID Regulator, in accordance with this rule, of the proposed engagement by the entity of a contractor to provide, on behalf of the entity, a service the entity is accredited to provide, or part of such a service, within the Australian Government Digital ID System.

Note: The accredited entity's DI data environment will include details of contractors providing an accredited service on behalf of the accredited entity.

(3) The notification must include the following information:

(a) the accredited services affected by the proposed engagement;

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

(i) the name of the incoming contractor;

(ii) the incoming contractor's 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; and

(v) the business name or names of the incoming contractor;

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

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

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

(f) 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, the Accreditation Rules, the Digital ID Data Standards or service levels.

(4) The notification must be made no later than 28 days before the engagement is proposed to start.

(4A) Subrule (4) does not apply if:

(a) there is a material change in the entity's circumstances (***change in circumstances***) that might affect the entity's ability to comply with its obligations under the Act, these rules, the Accreditation Rules, the Digital ID Data Standards or service levels;

(b) the proposed engagement is necessary to manage the change in circumstances;

(c) as a result of the change in circumstances, the entity is unable to comply with the timeframe specified in subrule (4); and

(d) the notification required by this rule is made at the same time, or before, the entity complies with rule 4.5 in relation to the change in circumstances.

Note: A person who wishes to rely on this subrule bears an evidential burden in relation to the matters mentioned in this subrule (see section 96 of the Regulatory Powers Act).

(5) Subrule (1) does not apply if the proposal to engage the incoming contractor has previously been notified to the Digital ID Regulator, including in the entity's application for approval to participate.

(6) In this rule:

ABN has the meaning given in section 9 of the Corporations Act.

ARBN has the meaning given in section 9 of the Corporations Act.

4.5 Other incidents

(1) This rule applies to:

(a) a participating entity; and

(b) an entity whose approval to participate is suspended;

in respect of incidents that have occurred, or are reasonably suspected of having occurred, while the entity was participating in the Australian Government Digital ID System.

(2) The entity must notify the Digital ID Regulator, in accordance with this rule, of the following incidents:

(a) any material change in the entity's circumstances that might affect its ability to comply with its obligations under the Act, these rules, the Accreditation Rules, the Digital ID Data Standards or service levels;

(b) any matter that could be relevant to a decision as to whether the entity is, having regard to the matters specified in Chapter 2 of these rules, a fit and proper person to be approved to participate, including matters involving an associated person of the entity; and

(c) any material change to, or error in, any of the information provided to the Digital ID Regulator.

(3) If the entity is an accredited entity—the entity must notify the System Administrator, in accordance with this rule, of the following incidents:

(a) any proposed change to the entity's information technology system that interacts with the Australian Government Digital ID System, where the change will, or could reasonably be expected to, have a material effect on the operation of the Australian Government Digital ID System; and

(b) any planned or unplanned outage or downtime affecting the entity's information technology system, where the outage or downtime will, or could reasonably be expected to, have a material effect on the operation of the Australian Government Digital ID System.

(4) The notification must include the following information:

(a) the entity's name;

(b) the contact details for the entity;

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

(d) a description of the incident;

(e) the following details of the incident:

(i) the date and time of the incident;

(ii) the date on which the entity became aware of the incident; and

(f) if subrule (2) applies—sufficient other details of the incident to enable the Digital ID Regulator to determine whether the Regulator should take any action in relation to the entity's approval to participate.

(5) The notification must be made no later than 5 business days after the entity becomes aware of the incident or a suspected incident.

4.6 Other digital ID systems

(1) This rule applies to:

(a) an accredited entity that holds an approval to participate; and

(b) an accredited entity whose approval to participate is suspended.

(2) The entity must notify the Digital ID Regulator, in accordance with this rule, if:

(a) the entity uses an information technology system to provide services within the Australian Government Digital ID System; and

(b) the entity proposes to use that information technology system to provide or receive services within a digital ID system (***other digital ID system***) other than the Australian Government Digital ID System.

(3) The notification must include the following information:

(a) the entity's name;

(b) the contact details for the entity;

(c) a description of:

(i) the services to be provided or received by the entity within the other digital ID system; and

(ii) any accredited services provided by the entity that are the same as or similar to the services to be provided or received by the entity within the other digital ID system;

(d) details of the entity providing or managing the other digital ID system;

(e) the nature of the proposed use of the other digital ID system;

(f) the likely effect of the entity's use of the other digital ID system on the levels of the entity's risk of:

(i) a cyber security incident; and

(ii) a digital ID fraud incident; and

(g) details of how the entity:

(i) will clearly distinguish information flows within the Australian Government Digital ID System from information flows within the other digital ID system;

(ii) will clearly distinguish between accredited services provided in the Australian Government Digital ID System and services provided within the other digital ID system;

(iii) will ensure that information held by the entity for the purposes of the Australian Government Digital ID System is able to be located and distinguished from information held by the entity for the purposes of the other digital ID system; and

(iv) will be able to meet its obligations under the Act, these rules, the Accreditation Rules, the Digital ID Data Standards and service levels in respect of its accredited services.

Example: For subparagraphs (g)(i) and (ii), an information barrier.

(4) The notification must be made no later than 28 days before the proposed use of the other digital ID system.

(5) In this rule:

other digital ID system has the meaning given in paragraph (2)(b).

4.7 System Administrator may disclose information

(1) The System Administrator may give information notified to it under rule 4.2 or subrule 4.5(3) to the Digital ID Regulator, the Minister or to a participating entity.

Note: These notifications relate to cyber security incidents and digital ID fraud incidents, proposed changes to the entity's information technology system and planned or unplanned outages or downtime affecting the entity's information technology system.

[Consultation note: This subrule is intended to allow for the Digital ID Regulator and the Minister to receive information held by the System Administrator, including information received from entities participating in the Australian Government Digital ID System (AGDIS), where it is appropriate and necessary for the Digital ID Regulator or the Minister to perform their functions. This includes in relation to the Digital ID Regulator's functions to oversee and maintain the AGDIS as well as ensure regulated entities remain in compliance with their obligations. It also enables the System Administrator to coordinate responses to incidents with entities in the AGDIS, which could include facilitating some information sharing to ensure users affected by an incident are supported by the entity best positioned to assist. Further amendments to this subrule may occur to support this intended purpose.]

(2) If the System Administrator acquires information about a cyber security incident or a digital ID fraud incident otherwise than by a notification under rule 4.2 or subrule 4.5(3), the System Administrator may give the information to a participating entity.

(3) The System Administrator may only give information under this rule if it considers it appropriate to do so to protect the security, integrity or performance of the Australian Government Digital ID System.

Note: This subrule does not limit the functions of the System Administrator under the Act, which include sharing information with the Minister, the Digital ID Regulator, the Digital ID Data Standards Chair and the Information Commissioner to assist them to exercise their powers or perform their functions under the Act (see subsection 95(i) of the Act).

(4) For the purposes of paragraph 78(2)(g) of the Act, a person or body to whom the System Administrator may disclose information under this rule is authorised to collect the information.

Note: This rule does not limit the functions of the Digital ID Regulator under the Act, which include sharing information with the Minister, the System Administrator, the Digital ID Data Standards Chair and the Information Commissioner to assist them to exercise their powers or perform their functions under the Act (see subsection 91(f) of the Act).

Chapter 5—Trustmarks

5.1 Application of this Chapter

(1)For the purposes of subsection 117(1) of the Act, this Chapter specifies the digital ID trustmark that may be used by an accredited entity and the conditions in relation to the use or display of that digital ID trustmark.

Note: An entity is liable to a civil penalty if:

(a) an entity uses a digital ID trustmark, but the entity is not authorised by these rules to use the digital ID trustmark (see subsection 118(2) of the Act); or

(b) an entity is required by these rules to display a digital ID trustmark in circumstances specified in these and the entity fails to comply with the requirement (see section 119 of the Act).

(2)To avoid doubt, this Chapter does not affect any right arising under the *Trade Marks Act 1995* or the *Designs Act 2003* in respect of a digital ID trustmark or an element of a digital ID trustmark.

(3)In this Chapter:

Australia's Digital ID System Accreditation Mark has the meaning given by rule 5.2.

5.2 Digital ID trustmark

The digital ID trustmark (***Australia's Digital ID System Accreditation Mark***) specified in item 1 of Schedule 1 may be used by an accredited entity.

5.3 Conditions in relation to use or display of digital ID trustmark

(1)This rule prescribes the conditions and requirements in relation to the use or display of the Australia's Digital ID System Accreditation Mark by an accredited entity.

Accredited identity exchange providers

(2)The Australia's Digital ID System Accreditation Mark may only be used or displayed by an accredited identity exchange provider:

(a)on public-facing accredited services that an individual must use to access the accredited services of the accredited identity exchange provider;

(b)on any document that contains public-facing information related to accredited services concerning:

(i)the accredited services of the accredited identity exchange provider; or

(ii)the accredited services of another accredited entity that is operating within the same digital ID system as the accredited services of the accredited identity exchange provider.

Example: Subparagraph (2)(b)(ii) would allow an accredited identity exchange provider to publish a list of its service providers and identify which of those providers are accredited entities by using the Australia's Digital ID System Accreditation Mark.

Accredited entities

(3)If an accredited entity uses or displays the Australia's Digital ID System Accreditation Mark, the accredited entity must also:

(a)use and display a hyperlink to the Digital ID Accredited Entities Register near the Australia's Digital ID System Accreditation Mark;

(b)if a document on which the Australia's Digital ID System Accreditation Mark is or can be printed—use and display the internet address of the Digital ID Accredited Entities Register near the Australia's Digital ID System Accreditation Mark; and

(c)if the accredited entity also provides a service that is not an accredited service—take reasonable steps to ensure when using or displaying the Australia's Digital ID System Accreditation Mark that it is clear which service is an accredited service and which service is not an accredited service.

(4)An entity ceases to be permitted to use or display a digital ID trustmark within 7 days of the entity's accreditation being suspended or revoked.

(5)In this rule:

document has the same meaning as in the *Acts Interpretations Act 1901*.

Example: A 'document' can include an electronic document, such as a webpage or mobile app, or a printed document.

Chapter 6—Record-keeping

6.1 Application of this Chapter

(1) For the purposes of subsection 135 of the Act, an entity specified in subrule (2) must keep records of the kind, for the period and in the manner prescribed by this Chapter.

(2) This Chapter applies to:
  (a) an accredited entity that holds an approval to participate in the Australian Government Digital ID System;
  (b) an accredited entity whose approval to participate in the Australian Government Digital ID System is suspended; and
  (c) an accredited entity whose approval to participate in the Australian Government Digital ID System has been revoked.

(3) For the avoidance of doubt, if the accreditation of an entity has been suspended or revoked, this Chapter continues to apply to the entity after its accreditation has been suspended or revoked.

6.2 Record keeping requirements for accredited entities

(1) An accredited entity must keep a prescribed record for the period that ends at the later of the following:
  (a) 6 years after the date the record was created;
  (b) 6 years after the record was last used by the entity for the purpose of providing a service that the entity is or was accredited to provide.

(2) An accredited entity must not destroy or de identify information contained in a prescribed record if:
  (a) the information is personal information; and
  (b) the information was obtained by the entity when providing its accredited services; and
  (c) the entity is required or authorised to retain the information by or under:
    (i) the Act, these rules or the Accreditation Rules;
    (ii) a direction issued by the Digital ID Regulator under section 127 of the Act; or
    (iii) a court/tribunal order (within the meaning of the Privacy Act); and
  (d) the information relates to any current or anticipated legal proceedings, dispute resolution proceedings or a current compliance or enforcement investigation under this Act, to which the entity is a party.

(3) In this rule:

prescribed record, in relation to an entity, means a record that:
  (a) is a log required by rule 4.20 of the Accreditation Rules; and
  (b) contains personal information.

Chapter 7—Interim liability arrangements

7.1 Simplified outline of this Chapter

This Chapter contains the interim liability arrangements for the commencement phase of the Australian Government Digital ID System established by the Act. Consistent with the arrangements that existed under the unlegislated scheme prior to the commencement of the Act (including with State and Territory government entities piloting the scheme), accredited entities participating in the Australian Government Digital ID System will have no liability to other parties to the statutory contract for anything done or omitted to be done within the Australian Government Digital ID Scheme.

It is expected that the interim liability arrangements in this Chapter will be reviewed at or before the next phase of participation in the Australian Government Digital ID System.

7.2 Breaches of the statutory contract

(1) For the purposes of paragraph 85(5)(a) of the Act, this rule prescribes the conduct that does not, and the circumstances that do not, constitute a breach of the statutory contract by an accredited entity.

(2) The following are prescribed for the purpose of this rule:
  (a) compliance by the accredited entity with the statutory contract;
  (b) non-compliance by the accredited entity with the statutory contract.

7.3 Limits on the kinds of losses or damages and amount of compensation

(1) For the purposes of paragraphs 85(5)(c) and (d) of the Act, this rule:
  (a) limits the kinds of losses or damages for which compensation may be payable by an accredited entity to another party (the ***other party***) to the statutory contract in relation to non-compliance by the accredited entity with the statutory contract; and
  (b) limits the amount of compensation that an accredited entity may be liable to pay the other party in relation to non-compliance by the accredited entity with the statutory contract.

(2) In relation to any non-compliance by the accredited entity with the statutory contract, no amount of compensation is payable to the other party in respect of any kinds of losses or damages:
  (a) directly or indirectly attributable to that non-compliance; or
  (b) for which compensation may otherwise be payable by the accredited entity to the other party apart from this rule.

Schedule 1—Digital ID trustmark

1 Digital ID trustmark for accredited entities

The following digital ID trustmark is specified for the purpose of subrule 5.2.

[*Insert image*]