Digital ID Rules 2024

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

Dated 7 November 2024

Katy Gallagher
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 the provisions in the Act in which the term 'Digital ID Rules' occurs.

1.4 Definitions

Note 1: A number of expressions used in these rules are defined in the Act, including the following:

(a) accredited entity;
(b) accredited service;
(c) cyber security incident;
(d) digital ID;
(e) participating relying party.

Note 2: A number of expressions used in these rules are defined in the Accreditation Rules, including the following:

(a) DI data environment;
(b) identity proofing level;
(c) public-facing accredited services;
(d) public-facing information related to accredited services.

(1) Unless otherwise specified, expressions defined in the Accreditation Rules have the same meaning in these rules.

(2) In these rules:

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

Accreditation Rules means the *Digital ID (Accreditation) Rules 2024*.

Act means the *Digital ID Act 2024*.

AGDIS Data Standards means the *Digital ID (AGDIS) Data Standards 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.

Corporations Act means the *Corporations Act 2001*.

IXP means an accredited identity exchange provider.

material change has its ordinary meaning.

Note: The definition of 'material change' in these rules is different to the definition of the same expression in the Accreditation Rules.

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.

pairwise identifier, in relation to an individual, means an identifier that:
(a) identifies the individual to an accredited entity or a participating relying party; and
(b) cannot be correlated with:
  (i) the individual's identifier used by a different accredited entity or participating relying party; or
  (ii) another individual's identifier.

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*.

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

Chapter 2—Fit and proper person considerations

2.1 Application of this Chapter

(1) For the purposes of paragraph 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 Accreditation Data Standards and the AGDIS Data Standards.

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 Accreditation Data Standards and the AGDIS Data Standards.

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 paragraphs 52(1A)(a) to (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 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;

Rule 2.2

(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 entity's 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 entity's application was refused;

(i) if the entity is or has been an accredited entity—whether the entity's 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 entity's 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.

director 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

For the purposes of paragraph 62(1)(f) of the Act, this Part prescribes additional requirements that must be met before the Digital ID Regulator may approve an entity to participate in the Australian Government Digital ID System.

Note: An application for approval to participate in the Australian Government Digital ID System 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

Before approving an application for approval to participate in the Australian Government Digital ID System, the Digital ID Regulator must be satisfied that the entity has in place effective written procedures to notify the System Administrator as soon as practicable of:

(a) any proposed change to the entity's information technology system that interacts with the Australian Government Digital ID System, if 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, if 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.

3.3 Applications for approval to participate—relying parties

(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 referred to 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) the frequency with which the entity will review the plan, being 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 referred to 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) the frequency with which the entity will review the plan, being 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) the frequency with which the entity will review the plan, being at least once per year.

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.

Participation conditions

Item	Column 1 Entity	Column 2 Condition
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	(a) The entity must notify the System Administrator, in accordance with subrule (2), of the following incidents that have occurred, or are reasonably suspected of having occurred: (i) any proposed change to the entity's information technology system that interacts with the Australian Government Digital ID System, if the change will, or could reasonably be expected to, have a material effect on the operation of the Australian Government Digital ID System; and (ii) any planned or unplanned outage or downtime affecting the entity's information technology system, if 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. (b) The notification must be made no later than 5 business days after the earliest of the following: (i) the entity becomes aware that the incident has occurred; or (ii) the entity reasonably suspects that the incident has occurred.
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).

(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; and

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

Chapter 4—Reportable incidents

4.1 Application of this Chapter

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;

if 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:
  (i) if the individual has been informed of the incident—when the individual was informed of the incident; and
  (ii) if the individual has not been informed of the incident—why the individual has not been informed of the incident;

(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 any action the entity has taken or will take to reduce the 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, the body or agency to which the incident was referred and the date and time of that referral; 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 that an incident has occurred or reasonably suspects an incident has occurred.

(5) The notification may be given orally. However, if it is given orally, a written notification must be given no later than 3 business days after the oral notification.

(6) If it is not reasonably practicable for the entity to provide some or all of the information required by subrule (3) (***required information***) 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) that includes as much of the required information as is reasonably available to the entity at the time the interim notification is given;

(b) takes reasonable steps to obtain the outstanding required information as soon as reasonably practicable; and

(c) provides any outstanding information as soon as reasonably practicable, and in any event within 48 hours of the outstanding information becoming available to the entity.

4.3 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 Accreditation Data Standards and the AGDIS Data Standards;

(b) any matter that could reasonably be considered relevant to whether the entity is a fit and proper person for the purposes of the Act, these rules, the Accreditation Rules, the Accreditation Data Standards and the AGDIS Data Standards, 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;

(d) a description of the incident; and

(e) the following details of the incident:

(i) the date and time of the incident; and

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

(5) The notification must be made no later than 5 business days after the earliest of the following:

(a) the entity becomes aware that the incident has occurred; or

(b) the entity reasonably suspects that the incident has occurred.

4.4 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 than the Australian Government Digital ID System (***other 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 meet its obligations under the Act, these rules, the Accreditation Rules, the Accreditation Data Standards and the AGDIS Data Standards 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).

4.5 System Administrator may give information

(1) The System Administrator may give information notified to it under rule 4.2 or subrule 4.3(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.

(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 4.3(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 give 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).

Rule 5.1

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 and requirements in relation to the use or display of that digital ID trustmark.

(2) For the purposes of paragraph 168(1)(b) of the Act, this Chapter also specifies the digital ID trustmark that may be used by an entity specified in rule 5.4 (***authorised 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 subsection 118(1) of the Act 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 rules and the entity fails to comply with the requirement (see section 119 of the Act).

(3) To avoid doubt, this Chapter does not affect or limit a right or remedy provided by any other law of the Commonwealth or a law of a State or Territory.

(4) In this Chapter:

authorised entity has the meaning given by subrule 5.1(2).

Digital ID Accreditation Trustmark has the meaning given by rule 5.2.

5.2 Digital ID trustmark

The digital ID trustmark (***Digital ID Accreditation Trustmark***) specified in item 1 of Schedule 1 may be used by an accredited entity and an authorised entity.

5.3 Use or display of digital ID trustmark—accredited entities

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

Accredited identity exchange providers

(2) The Digital ID Accreditation Trustmark may only be used or displayed by an IXP:

(a) on public-facing accredited services of the IXP;

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

(i) the accredited services of the IXP; or

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

Example: Subparagraph (2)(b)(ii) allows an IXP to publish a list of its service providers and identify which of those providers are accredited entities by using the Digital ID Accreditation Trustmark.

Accredited entities

(3) If an accredited entity uses or displays the Digital ID Accreditation Trustmark, the accredited entity must also:

(a) use and display a hyperlink to the Digital ID Accredited Entities Register near the Digital ID Accreditation Trustmark;

(b) if a document on which the Digital ID Accreditation Trustmark is or can be printed—use and display the internet address of the Digital ID Accredited Entities Register near the Digital ID Accreditation Trustmark; 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 Digital ID Accreditation Trustmark 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 the Digital ID Accreditation Trustmark within 7 days of the entity's accreditation being suspended or revoked.

5.4 Use or display of digital ID trustmark—authorised entities

(1) This rule prescribes the conditions in relation to the use or display of the Digital ID Accreditation Trustmark by an authorised entity.

(2) For the purposes of this rule, the following entities are authorised entities:

(a) the Digital ID Regulator;

(b) the System Administrator;

(c) the Information Commissioner; and

(d) the Secretary.

(3) The Digital ID Accreditation Trustmark may only be used or displayed by an authorised entity for the following purposes:

(a) the performance of functions under or in relation to the Act;

(b) education in relation to 'this Act' (as defined in section 9 of the Act);

(c) promotion of the objects of 'this Act' (as defined in section 9 of the Act).

Rule 6.1

Chapter 6—Record-keeping

6.1 Application of this Chapter

(1) For the purposes of subsection 135(3) 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) Subject to subrule (3), this Chapter applies to:
  (a) an entity that holds an approval to participate in the Australian Government Digital ID System;
  (b) an entity whose approval to participate in the Australian Government Digital ID System is suspended; and
  (c) an entity whose approval to participate in the Australian Government Digital ID System has been revoked.

(3) This Chapter does not apply to a relying party.

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

6.2 Record keeping requirements

(1) An entity must keep a prescribed record for whichever of the following periods ends later:
  (a) the period of 3 years that starts on the day the record was created;
  (b) the period of 3 years that starts on the day 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 entity must not destroy or de-identify information contained in a prescribed record if:
  (a) the information is personal information; and
  (b) the information is not biometric information; and
  (c) the information was obtained by the entity in the course of providing accredited services; and
  (d) 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
  (e) the information relates to:
    (i) any current or anticipated legal proceedings; or
    (ii) any dispute resolution proceedings; or
    (iii) a current compliance or enforcement investigation under ‘this Act’ (as defined in section 9 of the 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 subrule 4.20(7) of the Accreditation Rules; and

(b) contains personal information.

Item 1

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.