EXPOSURE DRAFT

Digital ID Amendment (Redress Framework and Other Measures) Rules 2025

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

Dated

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

Consultation draft

Contents

Consultation draft

EXPOSURE DRAFT

1 Name

This instrument is the *Digital ID Amendment (Redress Framework and Other Measures) Rules 2025*.

2 Commencement

(1) Each provision of this instrument 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	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. The whole of this instrument	The day after this instrument is registered.	

Note: This table relates only to the provisions of this instrument as originally made.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 this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

This instrument is made under section 168 of the *Digital ID Act 2024*.

4 Schedules

Each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

Consultation draft

EXPOSURE DRAFT

Schedule 1—Redress framework

Digital ID Rules 2024

1 After Chapter 4

Insert:

Chapter 4A—Redress framework

Part 1—Preliminary

4A.1 Application of this Chapter

(1) For the purposes of subsection 88(1) of the Act, this Chapter provides for a redress framework for incidents that occur in relation to accredited services of accredited entities that are provided within the Australian Government Digital ID System.

(2) This Chapter applies to an ASP or an ISP that is one of the following:
  (a) a participating entity;
  (b) an entity whose approval to participate is suspended;
  (c) an entity whose approval to participate has been revoked.

Note 1: This Chapter deals with cyber security incidents and digital ID fraud incidents that occur in certain circumstances. Rule 4.2 (Cyber security incidents and digital ID fraud incidents) of these rules and rules 4.11 (Support to individuals), 4.30 (Support to individuals) and 5.8 (Digital IDs affected by a fraud or cyber security incident) of the Accreditation Rules also deal with cyber security incidents and digital ID fraud incidents.

Note 2: Part 5 of this Chapter does not apply to an ASP or an ISP whose approval to participate is suspended or has been revoked (see rule 4A.6).

Part 2—Notifying affected individuals of incidents

4A.2 Notifying affected individuals of incidents

(1) If a cyber security incident or a digital ID fraud incident occurs, or is reasonably suspected of having occurred, in relation to an accredited service provided by an entity to which this Chapter applies within the Australian Government Digital ID System, the entity must:
  (a) consider whether it is appropriate to notify each individual affected by the incident; and
  (b) if the entity is satisfied that it is appropriate to notify a particular individual—make reasonable attempts to notify the individual.

Note: If an entity notifies an individual under paragraph (1)(b), the entity must also provide certain information, support and assistance to the individual (see rule 4A.5).

(2) In considering whether it is appropriate to notify an individual under paragraph (1)(a), the entity must consider the following:

Consultation draft

(a) the likelihood of the individual suffering an adverse outcome as a result of the incident or of the entity attempting to notify the individual of the incident;
(b) whether notifying the individual will, or could reasonably be expected to, have a material effect on the operation of the Australian Government Digital ID System.

Part 3—Referring unresolved technical issues to the System Administrator

4A.3 Unresolved technical issues must be referred to the System Administrator

(1) This rule applies if:
(a) a cyber security incident or a digital ID fraud incident occurs, or is reasonably suspected of having occurred, in relation to an accredited service provided by an entity to which this Chapter applies within the Australian Government Digital ID System; and
(b) as a result of the incident, an individual is unable to use their digital ID due to a technical issue with the entity's service that is within the control of the entity or another entity to which this Chapter applies.

(2) The entity must refer the technical issue to the System Administrator:
(a) as soon as reasonably practicable after the entity becomes aware of the issue; and
(b) if the entity became aware of the issue because of a complaint made by the individual—in any case within 28 days after the complaint is made.

(3) However, the entity must refer the issue to the System Administrator under subrule (2) only if:
(a) the entity is reasonably satisfied that the technical issue cannot be resolved without referring it to the System Administrator; and
(b) the entity has complied with rule 4A.5 (if applicable) in relation to the incident.

Note: Rule 4A.5 is applicable if the entity became aware of the issue because of a complaint made by the individual (see paragraph 4A.5(1)(b)).

4A.4 System Administrator may recommend a resolution

(1) If the System Administrator receives a referral from an entity under rule 4A.3, the System Administrator may recommend a course of action to the entity to resolve the technical issue.

(2) Without limiting subrule (1), a course of action recommended by the System Administrator may include that the entity do any of the following:
(a) provide the individual an explanation of the circumstances giving rise to the technical issue;
(b) issue an apology to the individual.

Consultation draft

Part 4—Providing information, support and assistance to individuals affected by incidents

4A.5 Providing information, support and assistance to individuals affected by incidents

(1) This rule applies if:

(a) an entity notifies an individual about an incident under paragraph 4A.2(1)(b); or

(b) an entity becomes aware of a technical issue mentioned in rule 4A.3 because of a complaint made by an individual.

(2) The entity must:

(a) direct the individual to any relevant public resources, including the information published by the entity on the resolution of incidents and the entity's complaints processes; and

(b) if the individual is unable to use their digital ID due to a technical issue with the entity's service that is within the control of another entity to which this Chapter applies—provide reasonable assistance to help the individual identify that other entity and its contact details.

Part 5—Policies relating to incidents and complaints

4A.6 Application of this Part

Despite subrule 4A.1(2), this Part does not apply to an ASP or an ISP that is one of the following:

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

(b) an entity whose approval to participate has been revoked.

4A.7 Policies relating to the identification etc. of incidents

An entity to which this Part applies must develop and publish policies relating to the identification, management and resolution of cyber security incidents and digital ID fraud incidents that occur, or are reasonably suspected of having occurred, in relation to the accredited services provided by the entity within the Australian Government Digital ID System.

4A.8 Policies relating to complaints by individuals

(1) An entity to which this Part applies must develop and publish policies relating to complaints by individuals relating to cyber security incidents and digital ID fraud incidents that occur, or are reasonably suspected of having occurred, in relation to the accredited services provided by the entity within the Australian Government Digital ID System.

(2) Without limiting subrule (1), the policies must deal with the following matters:

Consultation draft

(a) the process by which an individual may make a complaint to the entity, including the contact details that an individual may use for that purpose;
(b) procedures for dealing with complaints made by individuals and a simplified outline of those procedures;
(c) timeframes for resolving complaints made by individuals.

(3) An entity may comply with subrule (1) by developing and publishing a policy relating to complaints by individuals:
(a) generally; or
(b) in relation to other matters as well as the matters mentioned in subrules (1) and (2).

Consultation draft

EXPOSURE DRAFT

Schedule 2—Machinery of government changes

Digital ID Rules 2024

1 Subrule 1.4(2)

Insert:

receiving entity: see rule 1.5.

streamlined application: see rule 1.5.

transferring entity: see rule 1.5.

2 After rule 1.4

Insert:

1.5 Meaning of *streamlined application*

In these rules, ***streamlined application*** means an application under section 61 of the Act made by an entity (the ***receiving entity***) where:

(a) the receiving entity is of a kind mentioned in paragraph (c), (d), (e), (f) or (g) of the definition of ***entity*** in the Act; and

(b) a participating relying party (the ***transferring entity***) that is an entity of a kind mentioned in one of those paragraphs is approved to provide, or to provide access to, one or more services within the Australian Government Digital ID System (the ***approved services***); and

(c) a function of the transferring entity that includes the provision of the approved services is, or is reasonably expected to be, transferred to the receiving entity as a result of a machinery of government change; and

(d) the application is for an approval to provide, or to provide access to, one or more of the approved services.

3 Before subrule 2.2(1)

Insert:

(1A) This rule does not apply in relation to a streamlined application.

4 After rule 2.2

Insert:

2.3 Mandatory relevant matters—government entities affected by a machinery of government change

(1) This rule applies in relation to a streamlined application.

(2) In considering whether the receiving entity is a fit and proper person, the Digital ID Regulator must have regard to whether the approval of the corresponding transferring entity to provide, or to provide access to, services within the Australian Government Digital ID System, has ever been suspended or revoked.

Consultation draft

5 Rule 3.1 (after the heading)

Insert:

(1) This Part does not apply in relation to a streamlined application.

6 Rule 3.1

Before "For", insert "(2)".

Consultation draft

Schedule 3—Authorised entities for trustmarks

Digital ID Rules 2024

1 Paragraph 5.4(2)(c)

Omit "and".

2 At the end of subrule 5.4(2)

Add:

; (e) the Digital ID Data Standards Chair.

Consultation draft

Schedule 4—Reportable incidents

Digital ID Rules 2024

1 At the end of rule 4.2

Add:

(7) If the System Administrator receives a notification under subrule (2), the System Administrator may direct any entity of a kind mentioned in subrule (1) who has interacted with a digital ID affected by the incident to conduct an investigation into the incident.

(8) If the System Administrator directs an entity to conduct an investigation into an incident under subrule (7), that entity must:

(a) begin conducting the investigation as soon as reasonably practicable; and

(b) provide the System Administrator with a summary of the findings of the investigation as soon as reasonably practicable after the investigation is complete.

(9) However, if an investigation under subrule (7) is not completed within the period of 28 days beginning on the day the System Administrator directs the entity to conduct the investigation, the entity must update the System Administrator on the progress of the investigation:

(a) immediately after the end of that period; and

(b) at least once after the end of any subsequent period of 28 days until the investigation is complete.

Consultation draft

Schedule 5—Application, saving and transitional provisions

Digital ID Rules 2024

1 After Chapter 6

Insert:

Chapter 7—Application, saving and transitional provisions

7.1 Application of amendments made by the *Digital ID Amendment (Redress Framework and Other Measures) Rules 2025*

(1) In this rule:

amending Rules means the *Digital ID Amendment (Redress Framework and Other Measures) Rules 2025*.

commencement day means the day on which the amending Rules commence.

(2) Subrules 4.2(7), (8) and (9), as added by the amending Rules, apply in relation to notifications received on or after the commencement day.

(3) Rules 4A.2 and 4A.3, as inserted by the amending Rules, apply in relation to incidents that occur, or are reasonably suspected of having occurred, on or after the commencement day.

(4) Rules 4A.7 and 4A.8, as inserted by the amending Rules, apply to entities to which Part 5 of Chapter 4A applies on and after the end of the period of 6 months beginning on the commencement day.

Consultation draft